



참조 안내서

AWS 관리형 정책



AWS 관리형 정책: 참조 안내서

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

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 관련하여 고객에게 혼동을 일으킬 수 있는 방식이나 Amazon 브랜드 이미지를 떨어뜨리는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS 관리형 정책이란 무엇인가요?	1
정책 참조 페이지 이해	1
사용되지 않는 AWS 관리형 정책	2
AWS 관리형 정책	3
AccessAnalyzerServiceRolePolicy	44
이 정책 사용	44
정책 세부 정보	44
정책 버전	44
JSON 정책 문서	45
자세히 알아보기	47
AdministratorAccess	47
이 정책 사용	47
정책 세부 정보	47
정책 버전	48
JSON 정책 문서	48
자세히 알아보기	48
AdministratorAccess-Amplify	48
이 정책 사용	48
정책 세부 정보	49
정책 버전	49
JSON 정책 문서	49
자세히 알아보기	59
AdministratorAccess-AWSElasticBeanstalk	60
이 정책 사용	60
정책 세부 정보	60
정책 버전	60
JSON 정책 문서	60
자세히 알아보기	68
AlexaForBusinessDeviceSetup	69
이 정책 사용	69
정책 세부 정보	69
정책 버전	69
JSON 정책 문서	69
자세히 알아보기	70

AlexaForBusinessFullAccess	70
이 정책 사용	70
정책 세부 정보	70
정책 버전	71
JSON 정책 문서	71
자세히 알아보기	72
AlexaForBusinessGatewayExecution	72
이 정책 사용	72
정책 세부 정보	73
정책 버전	73
JSON 정책 문서	73
자세히 알아보기	74
AlexaForBusinessLifesizeDelegatedAccessPolicy	74
이 정책 사용	74
정책 세부 정보	74
정책 버전	75
JSON 정책 문서	75
자세히 알아보기	77
AlexaForBusinessNetworkProfileServicePolicy	77
이 정책 사용	77
정책 세부 정보	77
정책 버전	78
JSON 정책 문서	78
자세히 알아보기	79
AlexaForBusinessPolyDelegatedAccessPolicy	79
이 정책 사용	79
정책 세부 정보	79
정책 버전	79
JSON 정책 문서	79
자세히 알아보기	81
AlexaForBusinessReadOnlyAccess	81
이 정책 사용	82
정책 세부 정보	82
정책 버전	82
JSON 정책 문서	82
자세히 알아보기	82

AmazonAPIGatewayAdministrator	83
이 정책 사용	83
정책 세부 정보	83
정책 버전	83
JSON 정책 문서	83
자세히 알아보기	84
AmazonAPIGatewayInvokeFullAccess	84
이 정책 사용	84
정책 세부 정보	84
정책 버전	84
JSON 정책 문서	85
자세히 알아보기	85
AmazonAPIGatewayPushToCloudWatchLogs	85
이 정책 사용	85
정책 세부 정보	85
정책 버전	86
JSON 정책 문서	86
자세히 알아보기	86
AmazonAppFlowFullAccess	87
이 정책 사용	87
정책 세부 정보	87
정책 버전	87
JSON 정책 문서	87
자세히 알아보기	90
AmazonAppFlowReadOnlyAccess	90
이 정책 사용	90
정책 세부 정보	90
정책 버전	91
JSON 정책 문서	91
자세히 알아보기	91
AmazonAppStreamFullAccess	92
이 정책 사용	92
정책 세부 정보	92
정책 버전	92
JSON 정책 문서	92
자세히 알아보기	94

AmazonAppStreamPCAAccess	94
이 정책 사용	94
정책 세부 정보	94
정책 버전	95
JSON 정책 문서	95
자세히 알아보기	95
AmazonAppStreamReadOnlyAccess	96
이 정책 사용	96
정책 세부 정보	96
정책 버전	96
JSON 정책 문서	96
자세히 알아보기	97
AmazonAppStreamServiceAccess	97
이 정책 사용	97
정책 세부 정보	97
정책 버전	97
JSON 정책 문서	98
자세히 알아보기	99
AmazonAthenaFullAccess	99
이 정책 사용	99
정책 세부 정보	99
정책 버전	99
JSON 정책 문서	100
자세히 알아보기	103
AmazonAugmentedAIFullAccess	103
이 정책 사용	103
정책 세부 정보	103
정책 버전	104
JSON 정책 문서	104
자세히 알아보기	105
AmazonAugmentedAIHumanLoopFullAccess	105
이 정책 사용	105
정책 세부 정보	105
정책 버전	105
JSON 정책 문서	106
자세히 알아보기	106

AmazonAugmentedAllIntegratedAPIAccess	106
이 정책 사용	106
정책 세부 정보	107
정책 버전	107
JSON 정책 문서	107
자세히 알아보기	108
AmazonBedrockFullAccess	109
이 정책 사용	109
정책 세부 정보	109
정책 버전	109
JSON 정책 문서	109
자세히 알아보기	110
AmazonBedrockReadOnly	111
이 정책 사용	111
정책 세부 정보	111
정책 버전	111
JSON 정책 문서	111
자세히 알아보기	112
AmazonBraketFullAccess	112
이 정책 사용	112
정책 세부 정보	112
정책 버전	113
JSON 정책 문서	113
자세히 알아보기	117
AmazonBraketJobsExecutionPolicy	117
이 정책 사용	117
정책 세부 정보	117
정책 버전	118
JSON 정책 문서	118
자세히 알아보기	120
AmazonBraketServiceRolePolicy	120
이 정책 사용	121
정책 세부 정보	121
정책 버전	121
JSON 정책 문서	121
자세히 알아보기	122

AmazonChimeFullAccess	122
이 정책 사용	122
정책 세부 정보	122
정책 버전	122
JSON 정책 문서	123
자세히 알아보기	125
AmazonChimeReadOnly	125
이 정책 사용	125
정책 세부 정보	125
정책 버전	125
JSON 정책 문서	126
자세히 알아보기	126
AmazonChimeSDK	126
이 정책 사용	126
정책 세부 정보	126
정책 버전	127
JSON 정책 문서	127
자세히 알아보기	128
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	128
이 정책 사용	128
정책 세부 정보	128
정책 버전	129
JSON 정책 문서	129
자세히 알아보기	130
AmazonChimeSDKMessagingServiceRolePolicy	130
이 정책 사용	130
정책 세부 정보	130
정책 버전	131
JSON 정책 문서	131
자세히 알아보기	132
AmazonChimeServiceRolePolicy	132
이 정책 사용	132
정책 세부 정보	132
정책 버전	132
JSON 정책 문서	132
자세히 알아보기	133

AmazonChimeTranscriptionServiceLinkedRolePolicy	133
이 정책 사용	133
정책 세부 정보	133
정책 버전	134
JSON 정책 문서	134
자세히 알아보기	134
AmazonChimeUserManagement	134
이 정책 사용	135
정책 세부 정보	135
정책 버전	135
JSON 정책 문서	135
자세히 알아보기	136
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	136
이 정책 사용	137
정책 세부 정보	137
정책 버전	137
JSON 정책 문서	137
자세히 알아보기	139
AmazonCloudDirectoryFullAccess	139
이 정책 사용	139
정책 세부 정보	139
정책 버전	140
JSON 정책 문서	140
자세히 알아보기	140
AmazonCloudDirectoryReadOnlyAccess	140
이 정책 사용	141
정책 세부 정보	141
정책 버전	141
JSON 정책 문서	141
자세히 알아보기	142
AmazonCloudWatchEvidentlyFullAccess	142
이 정책 사용	142
정책 세부 정보	142
정책 버전	142
JSON 정책 문서	142
자세히 알아보기	145

AmazonCloudWatchEvidentlyReadOnlyAccess	145
이 정책 사용	145
정책 세부 정보	145
정책 버전	146
JSON 정책 문서	146
자세히 알아보기	146
AmazonCloudWatchEvidentlyServiceRolePolicy	147
이 정책 사용	147
정책 세부 정보	147
정책 버전	147
JSON 정책 문서	147
자세히 알아보기	149
AmazonCloudWatchRUMFullAccess	149
이 정책 사용	149
정책 세부 정보	149
정책 버전	149
JSON 정책 문서	149
자세히 알아보기	152
AmazonCloudWatchRUMReadOnlyAccess	152
이 정책 사용	152
정책 세부 정보	152
정책 버전	153
JSON 정책 문서	153
자세히 알아보기	153
AmazonCloudWatchRUMServiceRolePolicy	153
이 정책 사용	154
정책 세부 정보	154
정책 버전	154
JSON 정책 문서	154
자세히 알아보기	155
AmazonCodeCatalystFullAccess	155
이 정책 사용	155
정책 세부 정보	155
정책 버전	155
JSON 정책 문서	156
자세히 알아보기	156

AmazonCodeCatalystReadOnlyAccess	157
이 정책 사용	157
정책 세부 정보	157
정책 버전	157
JSON 정책 문서	157
자세히 알아보기	158
AmazonCodeCatalystSupportAccess	158
이 정책 사용	158
정책 세부 정보	158
정책 버전	158
JSON 정책 문서	159
자세히 알아보기	159
AmazonCodeGuruProfilerAgentAccess	160
이 정책 사용	160
정책 세부 정보	160
정책 버전	160
JSON 정책 문서	160
자세히 알아보기	161
AmazonCodeGuruProfilerFullAccess	161
이 정책 사용	161
정책 세부 정보	161
정책 버전	161
JSON 정책 문서	161
자세히 알아보기	162
AmazonCodeGuruProfilerReadOnlyAccess	162
이 정책 사용	163
정책 세부 정보	163
정책 버전	163
JSON 정책 문서	163
자세히 알아보기	164
AmazonCodeGuruReviewerFullAccess	164
이 정책 사용	164
정책 세부 정보	164
정책 버전	164
JSON 정책 문서	164
자세히 알아보기	167

AmazonCodeGuruReviewerReadOnlyAccess	167
이 정책 사용	167
정책 세부 정보	167
정책 버전	168
JSON 정책 문서	168
자세히 알아보기	168
AmazonCodeGuruReviewerServiceRolePolicy	169
이 정책 사용	169
정책 세부 정보	169
정책 버전	169
JSON 정책 문서	169
자세히 알아보기	171
AmazonCodeGuruSecurityFullAccess	171
이 정책 사용	172
정책 세부 정보	172
정책 버전	172
JSON 정책 문서	172
자세히 알아보기	172
AmazonCodeGuruSecurityScanAccess	173
이 정책 사용	173
정책 세부 정보	173
정책 버전	173
JSON 정책 문서	173
자세히 알아보기	174
AmazonCognitoDeveloperAuthenticatedIdentities	174
이 정책 사용	174
정책 세부 정보	174
정책 버전	175
JSON 정책 문서	175
자세히 알아보기	175
AmazonCognitoIdpEmailServiceRolePolicy	175
이 정책 사용	176
정책 세부 정보	176
정책 버전	176
JSON 정책 문서	176
자세히 알아보기	177

AmazonCognitoDpServiceRolePolicy	177
이 정책 사용	177
정책 세부 정보	177
정책 버전	177
JSON 정책 문서	178
자세히 알아보기	178
AmazonCognitoPowerUser	178
이 정책 사용	178
정책 세부 정보	178
정책 버전	179
JSON 정책 문서	179
자세히 알아보기	180
AmazonCognitoReadOnly	180
이 정책 사용	180
정책 세부 정보	181
정책 버전	181
JSON 정책 문서	181
자세히 알아보기	182
AmazonCognitoUnAuthedIdentitiesSessionPolicy	182
이 정책 사용	182
정책 세부 정보	182
정책 버전	182
JSON 정책 문서	183
자세히 알아보기	183
AmazonCognitoUnauthenticatedIdentities	183
이 정책 사용	184
정책 세부 정보	184
정책 버전	184
JSON 정책 문서	184
자세히 알아보기	185
AmazonConnect_FullAccess	185
이 정책 사용	185
정책 세부 정보	185
정책 버전	185
JSON 정책 문서	185
자세히 알아보기	188

AmazonConnectCampaignsServiceLinkedRolePolicy	188
이 정책 사용	188
정책 세부 정보	189
정책 버전	189
JSON 정책 문서	189
자세히 알아보기	190
AmazonConnectReadOnlyAccess	190
이 정책 사용	190
정책 세부 정보	190
정책 버전	190
JSON 정책 문서	190
자세히 알아보기	191
AmazonConnectServiceLinkedRolePolicy	191
이 정책 사용	191
정책 세부 정보	191
정책 버전	192
JSON 정책 문서	192
자세히 알아보기	197
AmazonConnectSynchronizationServiceRolePolicy	197
이 정책 사용	197
정책 세부 정보	197
정책 버전	198
JSON 정책 문서	198
자세히 알아보기	200
AmazonConnectVoiceIDFullAccess	200
이 정책 사용	200
정책 세부 정보	200
정책 버전	200
JSON 정책 문서	201
자세히 알아보기	201
AmazonDataZoneDomainExecutionRolePolicy	201
이 정책 사용	201
정책 세부 정보	201
정책 버전	202
JSON 정책 문서	202
자세히 알아보기	205

AmazonDataZoneEnvironmentRolePermissionsBoundary	205
이 정책 사용	205
정책 세부 정보	205
정책 버전	205
JSON 정책 문서	206
자세히 알아보기	218
AmazonDataZoneFullAccess	219
이 정책 사용	219
정책 세부 정보	219
정책 버전	219
JSON 정책 문서	219
자세히 알아보기	223
AmazonDataZoneFullUserAccess	223
이 정책 사용	223
정책 세부 정보	223
정책 버전	223
JSON 정책 문서	224
자세히 알아보기	226
AmazonDataZoneGlueManageAccessRolePolicy	227
이 정책 사용	227
정책 세부 정보	227
정책 버전	227
JSON 정책 문서	227
자세히 알아보기	232
AmazonDataZonePortalFullAccessPolicy	232
이 정책 사용	233
정책 세부 정보	233
정책 버전	233
JSON 정책 문서	233
자세히 알아보기	233
AmazonDataZonePreviewConsoleFullAccess	234
이 정책 사용	234
정책 세부 정보	234
정책 버전	234
JSON 정책 문서	234
자세히 알아보기	236

AmazonDataZoneProjectDeploymentPermissionsBoundary	236
이 정책 사용	237
정책 세부 정보	237
정책 버전	237
JSON 정책 문서	237
자세히 알아보기	245
AmazonDataZoneProjectRolePermissionsBoundary	245
이 정책 사용	245
정책 세부 정보	246
정책 버전	246
JSON 정책 문서	246
자세히 알아보기	253
AmazonDataZoneRedshiftGlueProvisioningPolicy	253
이 정책 사용	254
정책 세부 정보	254
정책 버전	254
JSON 정책 문서	254
자세히 알아보기	262
AmazonDataZoneRedshiftManageAccessRolePolicy	262
이 정책 사용	262
정책 세부 정보	262
정책 버전	262
JSON 정책 문서	263
자세히 알아보기	265
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary	265
이 정책 사용	265
정책 세부 정보	265
정책 버전	266
JSON 정책 문서	266
자세히 알아보기	293
AmazonDataZoneSageMakerManageAccessRolePolicy	293
이 정책 사용	293
정책 세부 정보	293
정책 버전	294
JSON 정책 문서	294
자세히 알아보기	298

AmazonDataZoneSageMakerProvisioningRolePolicy	299
이 정책 사용	299
정책 세부 정보	299
정책 버전	299
JSON 정책 문서	299
자세히 알아보기	304
AmazonDetectiveFullAccess	304
이 정책 사용	304
정책 세부 정보	304
정책 버전	305
JSON 정책 문서	305
자세히 알아보기	306
AmazonDetectiveInvestigatorAccess	306
이 정책 사용	306
정책 세부 정보	306
정책 버전	306
JSON 정책 문서	307
자세히 알아보기	308
AmazonDetectiveMemberAccess	308
이 정책 사용	309
정책 세부 정보	309
정책 버전	309
JSON 정책 문서	309
자세히 알아보기	310
AmazonDetectiveOrganizationsAccess	310
이 정책 사용	310
정책 세부 정보	310
정책 버전	310
JSON 정책 문서	311
자세히 알아보기	312
AmazonDetectiveServiceLinkedRolePolicy	312
이 정책 사용	313
정책 세부 정보	313
정책 버전	313
JSON 정책 문서	313
자세히 알아보기	314

AmazonDevOpsGuruConsoleFullAccess	314
이 정책 사용	314
정책 세부 정보	314
정책 버전	314
JSON 정책 문서	314
자세히 알아보기	317
AmazonDevOpsGuruFullAccess	317
이 정책 사용	317
정책 세부 정보	317
정책 버전	317
JSON 정책 문서	318
자세히 알아보기	320
AmazonDevOpsGuruOrganizationsAccess	320
이 정책 사용	320
정책 세부 정보	320
정책 버전	321
JSON 정책 문서	321
자세히 알아보기	322
AmazonDevOpsGuruReadOnlyAccess	322
이 정책 사용	322
정책 세부 정보	322
정책 버전	323
JSON 정책 문서	323
자세히 알아보기	325
AmazonDevOpsGuruServiceRolePolicy	325
이 정책 사용	325
정책 세부 정보	325
정책 버전	325
JSON 정책 문서	326
자세히 알아보기	330
AmazonDMSCloudWatchLogsRole	330
이 정책 사용	330
정책 세부 정보	330
정책 버전	330
JSON 정책 문서	330
자세히 알아보기	332

AmazonDMSRedshiftS3Role	332
이 정책 사용	332
정책 세부 정보	332
정책 버전	333
JSON 정책 문서	333
자세히 알아보기	333
AmazonDMSVPCManagementRole	334
이 정책 사용	334
정책 세부 정보	334
정책 버전	334
JSON 정책 문서	334
자세히 알아보기	335
AmazonDocDB-ElasticServiceRolePolicy	335
이 정책 사용	335
정책 세부 정보	335
정책 버전	336
JSON 정책 문서	336
자세히 알아보기	336
AmazonDocDBConsoleFullAccess	336
이 정책 사용	337
정책 세부 정보	337
정책 버전	337
JSON 정책 문서	337
자세히 알아보기	341
AmazonDocDBElasticFullAccess	342
이 정책 사용	342
정책 세부 정보	342
정책 버전	342
JSON 정책 문서	342
자세히 알아보기	345
AmazonDocDBElasticReadOnlyAccess	345
이 정책 사용	345
정책 세부 정보	346
정책 버전	346
JSON 정책 문서	346
자세히 알아보기	347

AmazonDocDBFullAccess	347
이 정책 사용	347
정책 세부 정보	347
정책 버전	347
JSON 정책 문서	348
자세히 알아보기	350
AmazonDocDBReadOnlyAccess	350
이 정책 사용	351
정책 세부 정보	351
정책 버전	351
JSON 정책 문서	351
자세히 알아보기	353
AmazonDRSVPCManagement	353
이 정책 사용	353
정책 세부 정보	353
정책 버전	354
JSON 정책 문서	354
자세히 알아보기	354
AmazonDynamoDBFullAccess	355
이 정책 사용	355
정책 세부 정보	355
정책 버전	355
JSON 정책 문서	355
자세히 알아보기	358
AmazonDynamoDBFullAccesswithDataPipeline	358
이 정책 사용	358
정책 세부 정보	358
정책 버전	359
JSON 정책 문서	359
자세히 알아보기	361
AmazonDynamoDBReadOnlyAccess	361
이 정책 사용	361
정책 세부 정보	361
정책 버전	361
JSON 정책 문서	362
자세히 알아보기	363

AmazonEBSCSIDriverPolicy	364
이 정책 사용	364
정책 세부 정보	364
정책 버전	364
JSON 정책 문서	364
자세히 알아보기	367
AmazonEC2ContainerRegistryFullAccess	368
이 정책 사용	368
정책 세부 정보	368
정책 버전	368
JSON 정책 문서	368
자세히 알아보기	369
AmazonEC2ContainerRegistryPowerUser	369
이 정책 사용	369
정책 세부 정보	369
정책 버전	370
JSON 정책 문서	370
자세히 알아보기	370
AmazonEC2ContainerRegistryReadOnly	371
이 정책 사용	371
정책 세부 정보	371
정책 버전	371
JSON 정책 문서	371
자세히 알아보기	372
AmazonEC2ContainerServiceAutoscaleRole	372
이 정책 사용	372
정책 세부 정보	372
정책 버전	373
JSON 정책 문서	373
자세히 알아보기	373
AmazonEC2ContainerServiceEventsRole	374
이 정책 사용	374
정책 세부 정보	374
정책 버전	374
JSON 정책 문서	374
자세히 알아보기	375

AmazonEC2ContainerServiceforEC2Role	375
이 정책 사용	376
정책 세부 정보	376
정책 버전	376
JSON 정책 문서	376
자세히 알아보기	377
AmazonEC2ContainerServiceRole	377
이 정책 사용	377
정책 세부 정보	378
정책 버전	378
JSON 정책 문서	378
자세히 알아보기	378
AmazonEC2FullAccess	379
이 정책 사용	379
정책 세부 정보	379
정책 버전	379
JSON 정책 문서	379
자세히 알아보기	380
AmazonEC2ReadOnlyAccess	381
이 정책 사용	381
정책 세부 정보	381
정책 버전	381
JSON 정책 문서	381
자세히 알아보기	382
AmazonEC2RoleforAWSCodeDeploy	382
이 정책 사용	382
정책 세부 정보	382
정책 버전	383
JSON 정책 문서	383
자세히 알아보기	383
AmazonEC2RoleforAWSCodeDeployLimited	384
이 정책 사용	384
정책 세부 정보	384
정책 버전	384
JSON 정책 문서	384
자세히 알아보기	385

AmazonEC2RoleforDataPipelineRole	385
이 정책 사용	385
정책 세부 정보	385
정책 버전	386
JSON 정책 문서	386
자세히 알아보기	387
AmazonEC2RoleforSSM	387
이 정책 사용	387
정책 세부 정보	387
정책 버전	387
JSON 정책 문서	388
자세히 알아보기	390
AmazonEC2RolePolicyForLaunchWizard	390
이 정책 사용	390
정책 세부 정보	390
정책 버전	390
JSON 정책 문서	391
자세히 알아보기	395
AmazonEC2SpotFleetAutoscaleRole	395
이 정책 사용	395
정책 세부 정보	395
정책 버전	395
JSON 정책 문서	395
자세히 알아보기	396
AmazonEC2SpotFleetTaggingRole	397
이 정책 사용	397
정책 세부 정보	397
정책 버전	397
JSON 정책 문서	397
자세히 알아보기	399
AmazonECS_FullAccess	399
이 정책 사용	399
정책 세부 정보	399
정책 버전	399
JSON 정책 문서	399
자세히 알아보기	405

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	405
이 정책 사용	405
정책 세부 정보	405
정책 버전	406
JSON 정책 문서	406
자세히 알아보기	408
AmazonECSInfrastructureRolePolicyForVolumes	408
이 정책 사용	408
정책 세부 정보	408
정책 버전	409
JSON 정책 문서	409
자세히 알아보기	411
AmazonECSServiceRolePolicy	411
이 정책 사용	411
정책 세부 정보	411
정책 버전	411
JSON 정책 문서	412
자세히 알아보기	416
AmazonECSTaskExecutionRolePolicy	417
이 정책 사용	417
정책 세부 정보	417
정책 버전	417
JSON 정책 문서	417
자세히 알아보기	418
AmazonEFSCSIDriverPolicy	418
이 정책 사용	418
정책 세부 정보	418
정책 버전	418
JSON 정책 문서	419
자세히 알아보기	420
AmazonEKS_CNI_Policy	420
이 정책 사용	421
정책 세부 정보	421
정책 버전	421
JSON 정책 문서	421
자세히 알아보기	422

AmazonEKSClusterPolicy	422
이 정책 사용	422
정책 세부 정보	422
정책 버전	423
JSON 정책 문서	423
자세히 알아보기	425
AmazonEKSConconnectorServiceRolePolicy	425
이 정책 사용	425
정책 세부 정보	425
정책 버전	426
JSON 정책 문서	426
자세히 알아보기	428
AmazonEKSFargatePodExecutionRolePolicy	428
이 정책 사용	428
정책 세부 정보	428
정책 버전	428
JSON 정책 문서	428
자세히 알아보기	429
AmazonEKSFForFargateServiceRolePolicy	429
이 정책 사용	429
정책 세부 정보	429
정책 버전	430
JSON 정책 문서	430
자세히 알아보기	430
AmazonEKSLocalOutpostClusterPolicy	430
이 정책 사용	431
정책 세부 정보	431
정책 버전	431
JSON 정책 문서	431
자세히 알아보기	433
AmazonEKSLocalOutpostServiceRolePolicy	433
이 정책 사용	433
정책 세부 정보	433
정책 버전	434
JSON 정책 문서	434
자세히 알아보기	439

AmazonEKSServicePolicy	439
이 정책 사용	440
정책 세부 정보	440
정책 버전	440
JSON 정책 문서	440
자세히 알아보기	442
AmazonEKSServiceRolePolicy	442
이 정책 사용	442
정책 세부 정보	442
정책 버전	442
JSON 정책 문서	443
자세히 알아보기	445
AmazonEKSVPCResourceController	445
이 정책 사용	445
정책 세부 정보	445
정책 버전	446
JSON 정책 문서	446
자세히 알아보기	446
AmazonEKSWorkerNodePolicy	447
이 정책 사용	447
정책 세부 정보	447
정책 버전	447
JSON 정책 문서	447
자세히 알아보기	448
AmazonElastiCacheFullAccess	448
이 정책 사용	448
정책 세부 정보	448
정책 버전	449
JSON 정책 문서	449
자세히 알아보기	452
AmazonElastiCacheReadOnlyAccess	452
이 정책 사용	452
정책 세부 정보	452
정책 버전	453
JSON 정책 문서	453
자세히 알아보기	453

AmazonElasticContainerRegistryPublicFullAccess	453
이 정책 사용	454
정책 세부 정보	454
정책 버전	454
JSON 정책 문서	454
자세히 알아보기	455
AmazonElasticContainerRegistryPublicPowerUser	455
이 정책 사용	455
정책 세부 정보	455
정책 버전	455
JSON 정책 문서	456
자세히 알아보기	456
AmazonElasticContainerRegistryPublicReadOnly	456
이 정책 사용	457
정책 세부 정보	457
정책 버전	457
JSON 정책 문서	457
자세히 알아보기	458
AmazonElasticFileSystemClientFullAccess	458
이 정책 사용	458
정책 세부 정보	458
정책 버전	458
JSON 정책 문서	459
자세히 알아보기	459
AmazonElasticFileSystemClientReadOnlyAccess	459
이 정책 사용	459
정책 세부 정보	459
정책 버전	460
JSON 정책 문서	460
자세히 알아보기	460
AmazonElasticFileSystemClientReadWriteAccess	460
이 정책 사용	461
정책 세부 정보	461
정책 버전	461
JSON 정책 문서	461
자세히 알아보기	462

AmazonElasticFileSystemFullAccess	462
이 정책 사용	462
정책 세부 정보	462
정책 버전	462
JSON 정책 문서	462
자세히 알아보기	464
AmazonElasticFileSystemReadOnlyAccess	464
이 정책 사용	464
정책 세부 정보	465
정책 버전	465
JSON 정책 문서	465
자세히 알아보기	466
AmazonElasticFileSystemServiceRolePolicy	466
이 정책 사용	466
정책 세부 정보	466
정책 버전	467
JSON 정책 문서	467
자세히 알아보기	469
AmazonElasticFileSystemsUtils	469
이 정책 사용	469
정책 세부 정보	469
정책 버전	469
JSON 정책 문서	470
자세히 알아보기	471
AmazonElasticMapReduceEditorsRole	472
이 정책 사용	472
정책 세부 정보	472
정책 버전	472
JSON 정책 문서	472
자세히 알아보기	473
AmazonElasticMapReduceforAutoScalingRole	474
이 정책 사용	474
정책 세부 정보	474
정책 버전	474
JSON 정책 문서	474
자세히 알아보기	475

AmazonElasticMapReduceforEC2Role	475
이 정책 사용	475
정책 세부 정보	475
정책 버전	475
JSON 정책 문서	476
자세히 알아보기	477
AmazonElasticMapReduceFullAccess	477
이 정책 사용	477
정책 세부 정보	477
정책 버전	478
JSON 정책 문서	478
자세히 알아보기	479
AmazonElasticMapReducePlacementGroupPolicy	480
이 정책 사용	480
정책 세부 정보	480
정책 버전	480
JSON 정책 문서	480
자세히 알아보기	481
AmazonElasticMapReduceReadOnlyAccess	481
이 정책 사용	481
정책 세부 정보	481
정책 버전	482
JSON 정책 문서	482
자세히 알아보기	482
AmazonElasticMapReduceRole	483
이 정책 사용	483
정책 세부 정보	483
정책 버전	483
JSON 정책 문서	483
자세히 알아보기	485
AmazonElasticsearchServiceRolePolicy	486
이 정책 사용	486
정책 세부 정보	486
정책 버전	486
JSON 정책 문서	486
자세히 알아보기	489

AmazonElasticTranscoder_FullAccess	489
이 정책 사용	489
정책 세부 정보	489
정책 버전	490
JSON 정책 문서	490
자세히 알아보기	491
AmazonElasticTranscoder_JobsSubmitter	491
이 정책 사용	491
정책 세부 정보	491
정책 버전	491
JSON 정책 문서	492
자세히 알아보기	492
AmazonElasticTranscoder_ReadOnlyAccess	492
이 정책 사용	492
정책 세부 정보	493
정책 버전	493
JSON 정책 문서	493
자세히 알아보기	493
AmazonElasticTranscoderRole	494
이 정책 사용	494
정책 세부 정보	494
정책 버전	494
JSON 정책 문서	494
자세히 알아보기	495
AmazonEMRCleanupPolicy	495
이 정책 사용	495
정책 세부 정보	496
정책 버전	496
JSON 정책 문서	496
자세히 알아보기	497
AmazonEMRContainersServiceRolePolicy	497
이 정책 사용	497
정책 세부 정보	497
정책 버전	497
JSON 정책 문서	498
자세히 알아보기	499

AmazonEMRFullAccessPolicy_v2	499
이 정책 사용	499
정책 세부 정보	499
정책 버전	499
JSON 정책 문서	500
자세히 알아보기	503
AmazonEMRReadOnlyAccessPolicy_v2	503
이 정책 사용	503
정책 세부 정보	503
정책 버전	504
JSON 정책 문서	504
자세히 알아보기	505
AmazonEMRServerlessServiceRolePolicy	505
이 정책 사용	505
정책 세부 정보	505
정책 버전	505
JSON 정책 문서	506
자세히 알아보기	507
AmazonEMRServicePolicy_v2	507
이 정책 사용	507
정책 세부 정보	507
정책 버전	507
JSON 정책 문서	507
자세히 알아보기	515
AmazonESCognitoAccess	515
이 정책 사용	515
정책 세부 정보	515
정책 버전	516
JSON 정책 문서	516
자세히 알아보기	517
AmazonESFullAccess	517
이 정책 사용	517
정책 세부 정보	517
정책 버전	517
JSON 정책 문서	518
자세히 알아보기	518

AmazonESReadOnlyAccess	518
이 정책 사용	518
정책 세부 정보	518
정책 버전	519
JSON 정책 문서	519
자세히 알아보기	519
AmazonEventBridgeApiDestinationsServiceRolePolicy	520
이 정책 사용	520
정책 세부 정보	520
정책 버전	520
JSON 정책 문서	520
자세히 알아보기	521
AmazonEventBridgeFullAccess	521
이 정책 사용	521
정책 세부 정보	521
정책 버전	521
JSON 정책 문서	522
자세히 알아보기	524
AmazonEventBridgePipesFullAccess	524
이 정책 사용	524
정책 세부 정보	524
정책 버전	524
JSON 정책 문서	524
자세히 알아보기	525
AmazonEventBridgePipesOperatorAccess	525
이 정책 사용	525
정책 세부 정보	526
정책 버전	526
JSON 정책 문서	526
자세히 알아보기	526
AmazonEventBridgePipesReadOnlyAccess	527
이 정책 사용	527
정책 세부 정보	527
정책 버전	527
JSON 정책 문서	527
자세히 알아보기	528

AmazonEventBridgeReadOnlyAccess	528
이 정책 사용	528
정책 세부 정보	528
정책 버전	528
JSON 정책 문서	529
자세히 알아보기	530
AmazonEventBridgeSchedulerFullAccess	530
이 정책 사용	530
정책 세부 정보	530
정책 버전	531
JSON 정책 문서	531
자세히 알아보기	531
AmazonEventBridgeSchedulerReadOnlyAccess	532
이 정책 사용	532
정책 세부 정보	532
정책 버전	532
JSON 정책 문서	532
자세히 알아보기	533
AmazonEventBridgeSchemasFullAccess	533
이 정책 사용	533
정책 세부 정보	533
정책 버전	533
JSON 정책 문서	534
자세히 알아보기	534
AmazonEventBridgeSchemasReadOnlyAccess	535
이 정책 사용	535
정책 세부 정보	535
정책 버전	535
JSON 정책 문서	535
자세히 알아보기	536
AmazonEventBridgeSchemasServiceRolePolicy	536
이 정책 사용	536
정책 세부 정보	536
정책 버전	537
JSON 정책 문서	537
자세히 알아보기	537

AmazonFISServiceRolePolicy	538
이 정책 사용	538
정책 세부 정보	538
정책 버전	538
JSON 정책 문서	538
자세히 알아보기	540
AmazonForecastFullAccess	540
이 정책 사용	540
정책 세부 정보	540
정책 버전	540
JSON 정책 문서	541
자세히 알아보기	541
AmazonFraudDetectorFullAccessPolicy	542
이 정책 사용	542
정책 세부 정보	542
정책 버전	542
JSON 정책 문서	542
자세히 알아보기	543
AmazonFreeRTOSFullAccess	544
이 정책 사용	544
정책 세부 정보	544
정책 버전	544
JSON 정책 문서	544
자세히 알아보기	545
AmazonFreeRTOSOTAUpdate	545
이 정책 사용	545
정책 세부 정보	545
정책 버전	545
JSON 정책 문서	545
자세히 알아보기	547
AmazonFSxConsoleFullAccess	547
이 정책 사용	547
정책 세부 정보	547
정책 버전	547
JSON 정책 문서	548
자세히 알아보기	551

AmazonFSxConsoleReadOnlyAccess	551
이 정책 사용	551
정책 세부 정보	551
정책 버전	552
JSON 정책 문서	552
자세히 알아보기	553
AmazonFSxFullAccess	553
이 정책 사용	553
정책 세부 정보	553
정책 버전	553
JSON 정책 문서	553
자세히 알아보기	557
AmazonFSxReadOnlyAccess	558
이 정책 사용	558
정책 세부 정보	558
정책 버전	558
JSON 정책 문서	558
자세히 알아보기	559
AmazonFSxServiceRolePolicy	559
이 정책 사용	559
정책 세부 정보	559
정책 버전	559
JSON 정책 문서	560
자세히 알아보기	562
AmazonGlacierFullAccess	562
이 정책 사용	563
정책 세부 정보	563
정책 버전	563
JSON 정책 문서	563
자세히 알아보기	563
AmazonGlacierReadOnlyAccess	564
이 정책 사용	564
정책 세부 정보	564
정책 버전	564
JSON 정책 문서	564
자세히 알아보기	565

AmazonGrafanaAthenaAccess	565
이 정책 사용	565
정책 세부 정보	565
정책 버전	566
JSON 정책 문서	566
자세히 알아보기	567
AmazonGrafanaCloudWatchAccess	568
이 정책 사용	568
정책 세부 정보	568
정책 버전	568
JSON 정책 문서	568
자세히 알아보기	570
AmazonGrafanaRedshiftAccess	570
이 정책 사용	570
정책 세부 정보	570
정책 버전	570
JSON 정책 문서	571
자세히 알아보기	572
AmazonGrafanaServiceLinkedRolePolicy	572
이 정책 사용	572
정책 세부 정보	572
정책 버전	573
JSON 정책 문서	573
자세히 알아보기	574
AmazonGuardDutyFullAccess	574
이 정책 사용	574
정책 세부 정보	574
정책 버전	575
JSON 정책 문서	575
자세히 알아보기	576
AmazonGuardDutyMalwareProtectionServiceRolePolicy	576
이 정책 사용	577
정책 세부 정보	577
정책 버전	577
JSON 정책 문서	577
자세히 알아보기	582

AmazonGuardDutyReadOnlyAccess	582
이 정책 사용	582
정책 세부 정보	582
정책 버전	582
JSON 정책 문서	582
자세히 알아보기	583
AmazonGuardDutyServiceRolePolicy	583
이 정책 사용	584
정책 세부 정보	584
정책 버전	584
JSON 정책 문서	584
자세히 알아보기	590
AmazonHealthLakeFullAccess	590
이 정책 사용	590
정책 세부 정보	590
정책 버전	591
JSON 정책 문서	591
자세히 알아보기	592
AmazonHealthLakeReadOnlyAccess	592
이 정책 사용	592
정책 세부 정보	592
정책 버전	592
JSON 정책 문서	592
자세히 알아보기	593
AmazonHoneycodeFullAccess	593
이 정책 사용	593
정책 세부 정보	593
정책 버전	594
JSON 정책 문서	594
자세히 알아보기	594
AmazonHoneycodeReadOnlyAccess	594
이 정책 사용	594
정책 세부 정보	595
정책 버전	595
JSON 정책 문서	595
자세히 알아보기	595

AmazonHoneycodeServiceRolePolicy	596
이 정책 사용	596
정책 세부 정보	596
정책 버전	596
JSON 정책 문서	596
자세히 알아보기	597
AmazonHoneycodeTeamAssociationFullAccess	597
이 정책 사용	597
정책 세부 정보	597
정책 버전	597
JSON 정책 문서	598
자세히 알아보기	598
AmazonHoneycodeTeamAssociationReadOnlyAccess	598
이 정책 사용	598
정책 세부 정보	598
정책 버전	599
JSON 정책 문서	599
자세히 알아보기	599
AmazonHoneycodeWorkbookFullAccess	599
이 정책 사용	600
정책 세부 정보	600
정책 버전	600
JSON 정책 문서	600
자세히 알아보기	601
AmazonHoneycodeWorkbookReadOnlyAccess	601
이 정책 사용	601
정책 세부 정보	601
정책 버전	601
JSON 정책 문서	602
자세히 알아보기	602
AmazonInspector2AgentlessServiceRolePolicy	602
이 정책 사용	603
정책 세부 정보	603
정책 버전	603
JSON 정책 문서	603
자세히 알아보기	607

AmazonInspector2FullAccess	607
이 정책 사용	607
정책 세부 정보	607
정책 버전	607
JSON 정책 문서	607
자세히 알아보기	609
AmazonInspector2ManagedCisPolicy	609
이 정책 사용	609
정책 세부 정보	609
정책 버전	609
JSON 정책 문서	610
자세히 알아보기	610
AmazonInspector2ReadOnlyAccess	610
이 정책 사용	610
정책 세부 정보	610
정책 버전	611
JSON 정책 문서	611
자세히 알아보기	612
AmazonInspector2ServiceRolePolicy	612
이 정책 사용	612
정책 세부 정보	612
정책 버전	612
JSON 정책 문서	612
자세히 알아보기	619
AmazonInspectorFullAccess	619
이 정책 사용	619
정책 세부 정보	619
정책 버전	619
JSON 정책 문서	620
자세히 알아보기	621
AmazonInspectorReadOnlyAccess	621
이 정책 사용	621
정책 세부 정보	621
정책 버전	621
JSON 정책 문서	622
자세히 알아보기	622

AmazonInspectorServiceRolePolicy	622
이 정책 사용	622
정책 세부 정보	623
정책 버전	623
JSON 정책 문서	623
자세히 알아보기	624
AmazonKendraFullAccess	624
이 정책 사용	625
정책 세부 정보	625
정책 버전	625
JSON 정책 문서	625
자세히 알아보기	627
AmazonKendraReadOnlyAccess	627
이 정책 사용	627
정책 세부 정보	627
정책 버전	628
JSON 정책 문서	628
자세히 알아보기	628
AmazonKeyspacesFullAccess	628
이 정책 사용	629
정책 세부 정보	629
정책 버전	629
JSON 정책 문서	629
자세히 알아보기	631
AmazonKeyspacesReadOnlyAccess	631
이 정책 사용	631
정책 세부 정보	631
정책 버전	632
JSON 정책 문서	632
자세히 알아보기	632
AmazonKeyspacesReadOnlyAccess_v2	633
이 정책 사용	633
정책 세부 정보	633
정책 버전	633
JSON 정책 문서	633
자세히 알아보기	634

AmazonKinesisAnalyticsFullAccess	634
이 정책 사용	635
정책 세부 정보	635
정책 버전	635
JSON 정책 문서	635
자세히 알아보기	636
AmazonKinesisAnalyticsReadOnly	637
이 정책 사용	637
정책 세부 정보	637
정책 버전	637
JSON 정책 문서	637
자세히 알아보기	639
AmazonKinesisFirehoseFullAccess	639
이 정책 사용	639
정책 세부 정보	639
정책 버전	639
JSON 정책 문서	639
자세히 알아보기	640
AmazonKinesisFirehoseReadOnlyAccess	640
이 정책 사용	640
정책 세부 정보	640
정책 버전	640
JSON 정책 문서	641
자세히 알아보기	641
AmazonKinesisFullAccess	641
이 정책 사용	641
정책 세부 정보	642
정책 버전	642
JSON 정책 문서	642
자세히 알아보기	642
AmazonKinesisReadOnlyAccess	643
이 정책 사용	643
정책 세부 정보	643
정책 버전	643
JSON 정책 문서	643
자세히 알아보기	644

AmazonKinesisVideoStreamsFullAccess	644
이 정책 사용	644
정책 세부 정보	644
정책 버전	644
JSON 정책 문서	645
자세히 알아보기	645
AmazonKinesisVideoStreamsReadOnlyAccess	645
이 정책 사용	645
정책 세부 정보	645
정책 버전	646
JSON 정책 문서	646
자세히 알아보기	646
AmazonLaunchWizard_Fullaccess	646
이 정책 사용	647
정책 세부 정보	647
정책 버전	647
JSON 정책 문서	647
자세히 알아보기	661
AmazonLaunchWizardFullAccessV2	661
이 정책 사용	662
정책 세부 정보	662
정책 버전	662
JSON 정책 문서	662
자세히 알아보기	679
AmazonLexChannelsAccess	679
이 정책 사용	679
정책 세부 정보	679
정책 버전	679
JSON 정책 문서	679
자세히 알아보기	680
AmazonLexFullAccess	680
이 정책 사용	680
정책 세부 정보	680
정책 버전	680
JSON 정책 문서	681
자세히 알아보기	686

AmazonLexReadOnly	686
이 정책 사용	686
정책 세부 정보	687
정책 버전	687
JSON 정책 문서	687
자세히 알아보기	688
AmazonLexReplicationPolicy	689
이 정책 사용	689
정책 세부 정보	689
정책 버전	689
JSON 정책 문서	689
자세히 알아보기	692
AmazonLexRunBotsOnly	692
이 정책 사용	692
정책 세부 정보	692
정책 버전	692
JSON 정책 문서	692
자세히 알아보기	693
AmazonLexV2BotPolicy	693
이 정책 사용	693
정책 세부 정보	693
정책 버전	694
JSON 정책 문서	694
자세히 알아보기	694
AmazonLookoutEquipmentFullAccess	694
이 정책 사용	694
정책 세부 정보	695
정책 버전	695
JSON 정책 문서	695
자세히 알아보기	696
AmazonLookoutEquipmentReadOnlyAccess	696
이 정책 사용	696
정책 세부 정보	697
정책 버전	697
JSON 정책 문서	697
자세히 알아보기	697

AmazonLookoutMetricsFullAccess	698
이 정책 사용	698
정책 세부 정보	698
정책 버전	698
JSON 정책 문서	698
자세히 알아보기	699
AmazonLookoutMetricsReadOnlyAccess	699
이 정책 사용	699
정책 세부 정보	699
정책 버전	700
JSON 정책 문서	700
자세히 알아보기	700
AmazonLookoutVisionConsoleFullAccess	701
이 정책 사용	701
정책 세부 정보	701
정책 버전	701
JSON 정책 문서	701
자세히 알아보기	703
AmazonLookoutVisionConsoleReadOnlyAccess	704
이 정책 사용	704
정책 세부 정보	704
정책 버전	704
JSON 정책 문서	704
자세히 알아보기	706
AmazonLookoutVisionFullAccess	706
이 정책 사용	706
정책 세부 정보	706
정책 버전	706
JSON 정책 문서	706
자세히 알아보기	707
AmazonLookoutVisionReadOnlyAccess	707
이 정책 사용	707
정책 세부 정보	707
정책 버전	708
JSON 정책 문서	708
자세히 알아보기	708

AmazonMachineLearningBatchPredictionsAccess	709
이 정책 사용	709
정책 세부 정보	709
정책 버전	709
JSON 정책 문서	709
자세히 알아보기	710
AmazonMachineLearningCreateOnlyAccess	710
이 정책 사용	710
정책 세부 정보	710
정책 버전	710
JSON 정책 문서	711
자세히 알아보기	711
AmazonMachineLearningFullAccess	711
이 정책 사용	711
정책 세부 정보	711
정책 버전	712
JSON 정책 문서	712
자세히 알아보기	712
AmazonMachineLearningManageRealTimeEndpointOnlyAccess	712
이 정책 사용	713
정책 세부 정보	713
정책 버전	713
JSON 정책 문서	713
자세히 알아보기	714
AmazonMachineLearningReadOnlyAccess	714
이 정책 사용	714
정책 세부 정보	714
정책 버전	714
JSON 정책 문서	714
자세히 알아보기	715
AmazonMachineLearningRealTimePredictionOnlyAccess	715
이 정책 사용	715
정책 세부 정보	715
정책 버전	716
JSON 정책 문서	716
자세히 알아보기	716

AmazonMachineLearningRoleforRedshiftDataSourceV3	716
이 정책 사용	717
정책 세부 정보	717
정책 버전	717
JSON 정책 문서	717
자세히 알아보기	718
AmazonMacieFullAccess	718
이 정책 사용	718
정책 세부 정보	718
정책 버전	719
JSON 정책 문서	719
자세히 알아보기	720
AmazonMacieHandshakeRole	720
이 정책 사용	720
정책 세부 정보	720
정책 버전	720
JSON 정책 문서	720
자세히 알아보기	721
AmazonMacieReadOnlyAccess	721
이 정책 사용	721
정책 세부 정보	721
정책 버전	722
JSON 정책 문서	722
자세히 알아보기	722
AmazonMacieServiceRole	722
이 정책 사용	723
정책 세부 정보	723
정책 버전	723
JSON 정책 문서	723
자세히 알아보기	723
AmazonMacieServiceRolePolicy	724
이 정책 사용	724
정책 세부 정보	724
정책 버전	724
JSON 정책 문서	724
자세히 알아보기	726

AmazonManagedBlockchainConsoleFullAccess	726
이 정책 사용	726
정책 세부 정보	726
정책 버전	726
JSON 정책 문서	726
자세히 알아보기	727
AmazonManagedBlockchainFullAccess	727
이 정책 사용	727
정책 세부 정보	727
정책 버전	728
JSON 정책 문서	728
자세히 알아보기	728
AmazonManagedBlockchainReadOnlyAccess	728
이 정책 사용	729
정책 세부 정보	729
정책 버전	729
JSON 정책 문서	729
자세히 알아보기	730
AmazonManagedBlockchainServiceRolePolicy	730
이 정책 사용	730
정책 세부 정보	730
정책 버전	730
JSON 정책 문서	731
자세히 알아보기	731
AmazonMCSFullAccess	731
이 정책 사용	731
정책 세부 정보	732
정책 버전	732
JSON 정책 문서	732
자세히 알아보기	733
AmazonMCSReadOnlyAccess	733
이 정책 사용	734
정책 세부 정보	734
정책 버전	734
JSON 정책 문서	734
자세히 알아보기	735

AmazonMechanicalTurkFullAccess	735
이 정책 사용	735
정책 세부 정보	735
정책 버전	735
JSON 정책 문서	736
자세히 알아보기	736
AmazonMechanicalTurkReadOnly	736
이 정책 사용	736
정책 세부 정보	736
정책 버전	737
JSON 정책 문서	737
자세히 알아보기	737
AmazonMemoryDBFullAccess	738
이 정책 사용	738
정책 세부 정보	738
정책 버전	738
JSON 정책 문서	738
자세히 알아보기	739
AmazonMemoryDBReadOnlyAccess	739
이 정책 사용	739
정책 세부 정보	739
정책 버전	740
JSON 정책 문서	740
자세히 알아보기	740
AmazonMobileAnalyticsFinancialReportAccess	740
이 정책 사용	741
정책 세부 정보	741
정책 버전	741
JSON 정책 문서	741
자세히 알아보기	741
AmazonMobileAnalyticsFullAccess	742
이 정책 사용	742
정책 세부 정보	742
정책 버전	742
JSON 정책 문서	742
자세히 알아보기	743

AmazonMobileAnalyticsNon-financialReportAccess	743
이 정책 사용	743
정책 세부 정보	743
정책 버전	743
JSON 정책 문서	744
자세히 알아보기	744
AmazonMobileAnalyticsWriteOnlyAccess	744
이 정책 사용	744
정책 세부 정보	744
정책 버전	745
JSON 정책 문서	745
자세히 알아보기	745
AmazonMonitronFullAccess	745
이 정책 사용	745
정책 세부 정보	746
정책 버전	746
JSON 정책 문서	746
자세히 알아보기	748
AmazonMQApiFullAccess	748
이 정책 사용	748
정책 세부 정보	748
정책 버전	748
JSON 정책 문서	749
자세히 알아보기	750
AmazonMQApiReadOnlyAccess	750
이 정책 사용	750
정책 세부 정보	750
정책 버전	750
JSON 정책 문서	751
자세히 알아보기	751
AmazonMQFullAccess	751
이 정책 사용	751
정책 세부 정보	751
정책 버전	752
JSON 정책 문서	752
자세히 알아보기	753

AmazonMQReadOnlyAccess	753
이 정책 사용	753
정책 세부 정보	753
정책 버전	754
JSON 정책 문서	754
자세히 알아보기	754
AmazonMQServiceRolePolicy	755
이 정책 사용	755
정책 세부 정보	755
정책 버전	755
JSON 정책 문서	755
자세히 알아보기	757
AmazonMSKConnectReadOnlyAccess	757
이 정책 사용	757
정책 세부 정보	757
정책 버전	758
JSON 정책 문서	758
자세히 알아보기	759
AmazonMSKFullAccess	759
이 정책 사용	759
정책 세부 정보	759
정책 버전	759
JSON 정책 문서	760
자세히 알아보기	762
AmazonMSKReadOnlyAccess	763
이 정책 사용	763
정책 세부 정보	763
정책 버전	763
JSON 정책 문서	763
자세히 알아보기	764
AmazonMWAAServiceRolePolicy	764
이 정책 사용	764
정책 세부 정보	764
정책 버전	764
JSON 정책 문서	765
자세히 알아보기	767

AmazonNimbleStudio-LaunchProfileWorker	767
이 정책 사용	767
정책 세부 정보	767
정책 버전	767
JSON 정책 문서	768
자세히 알아보기	768
AmazonNimbleStudio-StudioAdmin	769
이 정책 사용	769
정책 세부 정보	769
정책 버전	769
JSON 정책 문서	769
자세히 알아보기	771
AmazonNimbleStudio-StudioUser	771
이 정책 사용	771
정책 세부 정보	772
정책 버전	772
JSON 정책 문서	772
자세히 알아보기	774
AmazonOmicsFullAccess	774
이 정책 사용	774
정책 세부 정보	774
정책 버전	775
JSON 정책 문서	775
자세히 알아보기	776
AmazonOmicsReadOnlyAccess	776
이 정책 사용	776
정책 세부 정보	776
정책 버전	776
JSON 정책 문서	777
자세히 알아보기	777
AmazonOneEnterpriseFullAccess	777
이 정책 사용	777
정책 세부 정보	778
정책 버전	778
JSON 정책 문서	778
자세히 알아보기	778

AmazonOneEnterpriseInstallerAccess	779
이 정책 사용	779
정책 세부 정보	779
정책 버전	779
JSON 정책 문서	779
자세히 알아보기	780
AmazonOneEnterpriseReadOnlyAccess	780
이 정책 사용	780
정책 세부 정보	780
정책 버전	780
JSON 정책 문서	781
자세히 알아보기	781
AmazonOpenSearchDashboardsServiceRolePolicy	781
이 정책 사용	781
정책 세부 정보	781
정책 버전	782
JSON 정책 문서	782
자세히 알아보기	782
AmazonOpenSearchDirectQueryGlueCreateAccess	783
이 정책 사용	783
정책 세부 정보	783
정책 버전	783
JSON 정책 문서	783
자세히 알아보기	784
AmazonOpenSearchIngestionFullAccess	784
이 정책 사용	784
정책 세부 정보	784
정책 버전	784
JSON 정책 문서	785
자세히 알아보기	786
AmazonOpenSearchIngestionReadOnlyAccess	786
이 정책 사용	786
정책 세부 정보	786
정책 버전	786
JSON 정책 문서	786
자세히 알아보기	787

AmazonOpenSearchIngestionServiceRolePolicy	787
이 정책 사용	787
정책 세부 정보	787
정책 버전	788
JSON 정책 문서	788
자세히 알아보기	790
AmazonOpenSearchServerlessServiceRolePolicy	790
이 정책 사용	790
정책 세부 정보	790
정책 버전	790
JSON 정책 문서	790
자세히 알아보기	791
AmazonOpenSearchServiceCognitoAccess	791
이 정책 사용	791
정책 세부 정보	791
정책 버전	792
JSON 정책 문서	792
자세히 알아보기	793
AmazonOpenSearchServiceFullAccess	793
이 정책 사용	793
정책 세부 정보	793
정책 버전	793
JSON 정책 문서	794
자세히 알아보기	794
AmazonOpenSearchServiceReadOnlyAccess	794
이 정책 사용	794
정책 세부 정보	794
정책 버전	795
JSON 정책 문서	795
자세히 알아보기	795
AmazonOpenSearchServiceRolePolicy	796
이 정책 사용	796
정책 세부 정보	796
정책 버전	796
JSON 정책 문서	796
자세히 알아보기	801

AmazonPersonalizeFullAccess	801
이 정책 사용	801
정책 세부 정보	801
정책 버전	801
JSON 정책 문서	802
자세히 알아보기	803
AmazonPollyFullAccess	803
이 정책 사용	803
정책 세부 정보	803
정책 버전	803
JSON 정책 문서	804
자세히 알아보기	804
AmazonPollyReadOnlyAccess	804
이 정책 사용	804
정책 세부 정보	805
정책 버전	805
JSON 정책 문서	805
자세히 알아보기	805
AmazonPrometheusConsoleFullAccess	806
이 정책 사용	806
정책 세부 정보	806
정책 버전	806
JSON 정책 문서	806
자세히 알아보기	807
AmazonPrometheusFullAccess	808
이 정책 사용	808
정책 세부 정보	808
정책 버전	808
JSON 정책 문서	808
자세히 알아보기	809
AmazonPrometheusQueryAccess	809
이 정책 사용	810
정책 세부 정보	810
정책 버전	810
JSON 정책 문서	810
자세히 알아보기	811

AmazonPrometheusRemoteWriteAccess	811
이 정책 사용	811
정책 세부 정보	811
정책 버전	811
JSON 정책 문서	811
자세히 알아보기	812
AmazonPrometheusScrapperServiceRolePolicy	812
이 정책 사용	812
정책 세부 정보	812
정책 버전	813
JSON 정책 문서	813
자세히 알아보기	815
AmazonQFullAccess	815
이 정책 사용	815
정책 세부 정보	815
정책 버전	816
JSON 정책 문서	816
자세히 알아보기	816
AmazonQLDBConsoleFullAccess	817
이 정책 사용	817
정책 세부 정보	817
정책 버전	817
JSON 정책 문서	817
자세히 알아보기	819
AmazonQLDBFullAccess	819
이 정책 사용	819
정책 세부 정보	819
정책 버전	820
JSON 정책 문서	820
자세히 알아보기	821
AmazonQLDBReadOnly	821
이 정책 사용	821
정책 세부 정보	822
정책 버전	822
JSON 정책 문서	822
자세히 알아보기	823

AmazonRDSBetaServiceRolePolicy	823
이 정책 사용	823
정책 세부 정보	823
정책 버전	823
JSON 정책 문서	823
자세히 알아보기	827
AmazonRDSCustomInstanceProfileRolePolicy	827
이 정책 사용	827
정책 세부 정보	827
정책 버전	827
JSON 정책 문서	827
자세히 알아보기	835
AmazonRDSCustomPreviewServiceRolePolicy	835
이 정책 사용	835
정책 세부 정보	835
정책 버전	835
JSON 정책 문서	835
자세히 알아보기	851
AmazonRDSCustomServiceRolePolicy	851
이 정책 사용	851
정책 세부 정보	851
정책 버전	852
JSON 정책 문서	852
자세히 알아보기	869
AmazonRDSDataFullAccess	869
이 정책 사용	869
정책 세부 정보	870
정책 버전	870
JSON 정책 문서	870
자세히 알아보기	871
AmazonRDSDirectoryServiceAccess	871
이 정책 사용	871
정책 세부 정보	872
정책 버전	872
JSON 정책 문서	872
자세히 알아보기	872

AmazonRDSEnhancedMonitoringRole	873
이 정책 사용	873
정책 세부 정보	873
정책 버전	873
JSON 정책 문서	873
자세히 알아보기	874
AmazonRDSFullAccess	874
이 정책 사용	874
정책 세부 정보	874
정책 버전	875
JSON 정책 문서	875
자세히 알아보기	877
AmazonRDSPerformanceInsightsFullAccess	877
이 정책 사용	877
정책 세부 정보	877
정책 버전	878
JSON 정책 문서	878
자세히 알아보기	879
AmazonRDSPerformanceInsightsReadOnly	879
이 정책 사용	880
정책 세부 정보	880
정책 버전	880
JSON 정책 문서	880
자세히 알아보기	882
AmazonRDSPreviewServiceRolePolicy	882
이 정책 사용	882
정책 세부 정보	882
정책 버전	882
JSON 정책 문서	883
자세히 알아보기	886
AmazonRDSReadOnlyAccess	886
이 정책 사용	886
정책 세부 정보	886
정책 버전	886
JSON 정책 문서	887
자세히 알아보기	888

AmazonRDSServiceRolePolicy	888
이 정책 사용	888
정책 세부 정보	888
정책 버전	888
JSON 정책 문서	889
자세히 알아보기	893
AmazonRedshiftAllCommandsFullAccess	893
이 정책 사용	893
정책 세부 정보	893
정책 버전	893
JSON 정책 문서	893
자세히 알아보기	899
AmazonRedshiftDataFullAccess	899
이 정책 사용	899
정책 세부 정보	899
정책 버전	899
JSON 정책 문서	900
자세히 알아보기	902
AmazonRedshiftFullAccess	902
이 정책 사용	902
정책 세부 정보	902
정책 버전	902
JSON 정책 문서	902
자세히 알아보기	904
AmazonRedshiftQueryEditor	905
이 정책 사용	905
정책 세부 정보	905
정책 버전	905
JSON 정책 문서	905
자세히 알아보기	907
AmazonRedshiftQueryEditorV2FullAccess	907
이 정책 사용	908
정책 세부 정보	908
정책 버전	908
JSON 정책 문서	908
자세히 알아보기	909

AmazonRedshiftQueryEditorV2NoSharing	910
이 정책 사용	910
정책 세부 정보	910
정책 버전	910
JSON 정책 문서	910
자세히 알아보기	914
AmazonRedshiftQueryEditorV2ReadSharing	914
이 정책 사용	914
정책 세부 정보	914
정책 버전	915
JSON 정책 문서	915
자세히 알아보기	920
AmazonRedshiftQueryEditorV2ReadWriteSharing	920
이 정책 사용	920
정책 세부 정보	920
정책 버전	920
JSON 정책 문서	921
자세히 알아보기	926
AmazonRedshiftReadOnlyAccess	926
이 정책 사용	926
정책 세부 정보	926
정책 버전	926
JSON 정책 문서	927
자세히 알아보기	927
AmazonRedshiftServiceLinkedRolePolicy	927
이 정책 사용	928
정책 세부 정보	928
정책 버전	928
JSON 정책 문서	928
자세히 알아보기	933
AmazonRekognitionCustomLabelsFullAccess	934
이 정책 사용	934
정책 세부 정보	934
정책 버전	934
JSON 정책 문서	934
자세히 알아보기	936

AmazonRekognitionFullAccess	936
이 정책 사용	936
정책 세부 정보	936
정책 버전	936
JSON 정책 문서	936
자세히 알아보기	937
AmazonRekognitionReadOnlyAccess	937
이 정책 사용	937
정책 세부 정보	937
정책 버전	937
JSON 정책 문서	938
자세히 알아보기	939
AmazonRekognitionServiceRole	939
이 정책 사용	939
정책 세부 정보	939
정책 버전	939
JSON 정책 문서	940
자세히 알아보기	940
AmazonRoute53AutoNamingFullAccess	941
이 정책 사용	941
정책 세부 정보	941
정책 버전	941
JSON 정책 문서	941
자세히 알아보기	942
AmazonRoute53AutoNamingReadOnlyAccess	942
이 정책 사용	942
정책 세부 정보	942
정책 버전	943
JSON 정책 문서	943
자세히 알아보기	943
AmazonRoute53AutoNamingRegistrantAccess	943
이 정책 사용	944
정책 세부 정보	944
정책 버전	944
JSON 정책 문서	944
자세히 알아보기	945

AmazonRoute53DomainsFullAccess	945
이 정책 사용	945
정책 세부 정보	945
정책 버전	945
JSON 정책 문서	946
자세히 알아보기	946
AmazonRoute53DomainsReadOnlyAccess	946
이 정책 사용	946
정책 세부 정보	946
정책 버전	947
JSON 정책 문서	947
자세히 알아보기	947
AmazonRoute53FullAccess	948
이 정책 사용	948
정책 세부 정보	948
정책 버전	948
JSON 정책 문서	948
자세히 알아보기	949
AmazonRoute53ProfilesFullAccess	949
이 정책 사용	949
정책 세부 정보	949
정책 버전	950
JSON 정책 문서	950
자세히 알아보기	951
AmazonRoute53ProfilesReadOnlyAccess	951
이 정책 사용	951
정책 세부 정보	951
정책 버전	951
JSON 정책 문서	952
자세히 알아보기	952
AmazonRoute53ReadOnlyAccess	953
이 정책 사용	953
정책 세부 정보	953
정책 버전	953
JSON 정책 문서	953
자세히 알아보기	954

AmazonRoute53RecoveryClusterFullAccess	954
이 정책 사용	954
정책 세부 정보	954
정책 버전	954
JSON 정책 문서	955
자세히 알아보기	955
AmazonRoute53RecoveryClusterReadOnlyAccess	955
이 정책 사용	955
정책 세부 정보	955
정책 버전	956
JSON 정책 문서	956
자세히 알아보기	956
AmazonRoute53RecoveryControlConfigFullAccess	956
이 정책 사용	957
정책 세부 정보	957
정책 버전	957
JSON 정책 문서	957
자세히 알아보기	957
AmazonRoute53RecoveryControlConfigReadOnlyAccess	958
이 정책 사용	958
정책 세부 정보	958
정책 버전	958
JSON 정책 문서	958
자세히 알아보기	959
AmazonRoute53RecoveryReadinessFullAccess	959
이 정책 사용	959
정책 세부 정보	959
정책 버전	960
JSON 정책 문서	960
자세히 알아보기	960
AmazonRoute53RecoveryReadinessReadOnlyAccess	960
이 정책 사용	961
정책 세부 정보	961
정책 버전	961
JSON 정책 문서	961
자세히 알아보기	962

AmazonRoute53ResolverFullAccess	962
이 정책 사용	962
정책 세부 정보	962
정책 버전	963
JSON 정책 문서	963
자세히 알아보기	963
AmazonRoute53ResolverReadOnlyAccess	964
이 정책 사용	964
정책 세부 정보	964
정책 버전	964
JSON 정책 문서	964
자세히 알아보기	965
AmazonS3FullAccess	965
이 정책 사용	965
정책 세부 정보	965
정책 버전	965
JSON 정책 문서	966
자세히 알아보기	966
AmazonS3ObjectLambdaExecutionRolePolicy	966
이 정책 사용	966
정책 세부 정보	966
정책 버전	967
JSON 정책 문서	967
자세히 알아보기	967
AmazonS3OutpostsFullAccess	968
이 정책 사용	968
정책 세부 정보	968
정책 버전	968
JSON 정책 문서	968
자세히 알아보기	969
AmazonS3OutpostsReadOnlyAccess	969
이 정책 사용	970
정책 세부 정보	970
정책 버전	970
JSON 정책 문서	970
자세히 알아보기	971

AmazonS3ReadOnlyAccess	971
이 정책 사용	971
정책 세부 정보	972
정책 버전	972
JSON 정책 문서	972
자세히 알아보기	972
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	973
이 정책 사용	973
정책 세부 정보	973
정책 버전	973
JSON 정책 문서	973
자세히 알아보기	983
AmazonSageMakerCanvasAIServicesAccess	984
이 정책 사용	984
정책 세부 정보	984
정책 버전	984
JSON 정책 문서	984
자세히 알아보기	987
AmazonSageMakerCanvasBedrockAccess	987
이 정책 사용	988
정책 세부 정보	988
정책 버전	988
JSON 정책 문서	988
자세히 알아보기	989
AmazonSageMakerCanvasDataPrepFullAccess	989
이 정책 사용	989
정책 세부 정보	989
정책 버전	990
JSON 정책 문서	990
자세히 알아보기	997
AmazonSageMakerCanvasDirectDeployAccess	997
이 정책 사용	997
정책 세부 정보	997
정책 버전	997
JSON 정책 문서	998
자세히 알아보기	998

AmazonSageMakerCanvasForecastAccess	999
이 정책 사용	999
정책 세부 정보	999
정책 버전	999
JSON 정책 문서	999
자세히 알아보기	1000
AmazonSageMakerCanvasFullAccess	1000
이 정책 사용	1000
정책 세부 정보	1000
정책 버전	1001
JSON 정책 문서	1001
자세히 알아보기	1009
AmazonSageMakerClusterInstanceRolePolicy	1009
이 정책 사용	1009
정책 세부 정보	1009
정책 버전	1009
JSON 정책 문서	1010
자세히 알아보기	1011
AmazonSageMakerCoreServiceRolePolicy	1011
이 정책 사용	1012
정책 세부 정보	1012
정책 버전	1012
JSON 정책 문서	1012
자세히 알아보기	1013
AmazonSageMakerEdgeDeviceFleetPolicy	1013
이 정책 사용	1013
정책 세부 정보	1013
정책 버전	1014
JSON 정책 문서	1014
자세히 알아보기	1016
AmazonSageMakerFeatureStoreAccess	1016
이 정책 사용	1016
정책 세부 정보	1016
정책 버전	1016
JSON 정책 문서	1017
자세히 알아보기	1018

AmazonSageMakerFullAccess	1018
이 정책 사용	1018
정책 세부 정보	1018
정책 버전	1018
JSON 정책 문서	1018
자세히 알아보기	1034
AmazonSageMakerGeospatialExecutionRole	1035
이 정책 사용	1035
정책 세부 정보	1035
정책 버전	1035
JSON 정책 문서	1035
자세히 알아보기	1036
AmazonSageMakerGeospatialFullAccess	1036
이 정책 사용	1036
정책 세부 정보	1036
정책 버전	1037
JSON 정책 문서	1037
자세히 알아보기	1038
AmazonSageMakerGroundTruthExecution	1038
이 정책 사용	1038
정책 세부 정보	1038
정책 버전	1038
JSON 정책 문서	1038
자세히 알아보기	1042
AmazonSageMakerMechanicalTurkAccess	1042
이 정책 사용	1042
정책 세부 정보	1042
정책 버전	1043
JSON 정책 문서	1043
자세히 알아보기	1043
AmazonSageMakerModelGovernanceUseAccess	1043
이 정책 사용	1044
정책 세부 정보	1044
정책 버전	1044
JSON 정책 문서	1044
자세히 알아보기	1046

AmazonSageMakerModelRegistryFullAccess	1046
이 정책 사용	1046
정책 세부 정보	1046
정책 버전	1047
JSON 정책 문서	1047
자세히 알아보기	1050
AmazonSageMakerNotebooksServiceRolePolicy	1051
이 정책 사용	1051
정책 세부 정보	1051
정책 버전	1051
JSON 정책 문서	1051
자세히 알아보기	1055
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1055
이 정책 사용	1056
정책 세부 정보	1056
정책 버전	1056
JSON 정책 문서	1056
자세히 알아보기	1057
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1057
이 정책 사용	1057
정책 세부 정보	1058
정책 버전	1058
JSON 정책 문서	1058
자세히 알아보기	1061
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1062
이 정책 사용	1062
정책 세부 정보	1062
정책 버전	1062
JSON 정책 문서	1062
자세히 알아보기	1063
AmazonSageMakerPipelinesIntegrations	1063
이 정책 사용	1063
정책 세부 정보	1063
정책 버전	1064
JSON 정책 문서	1064
자세히 알아보기	1066

AmazonSageMakerReadOnly	1066
이 정책 사용	1066
정책 세부 정보	1066
정책 버전	1066
JSON 정책 문서	1067
자세히 알아보기	1068
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1068
이 정책 사용	1068
정책 세부 정보	1068
정책 버전	1069
JSON 정책 문서	1069
자세히 알아보기	1070
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1070
이 정책 사용	1070
정책 세부 정보	1070
정책 버전	1070
JSON 정책 문서	1071
자세히 알아보기	1077
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1078
이 정책 사용	1078
정책 세부 정보	1078
정책 버전	1078
JSON 정책 문서	1078
자세히 알아보기	1088
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1089
이 정책 사용	1089
정책 세부 정보	1089
정책 버전	1089
JSON 정책 문서	1089
자세히 알아보기	1092
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1092
이 정책 사용	1093
정책 세부 정보	1093
정책 버전	1093
JSON 정책 문서	1093
자세히 알아보기	1093

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1094
이 정책 사용	1094
정책 세부 정보	1094
정책 버전	1094
JSON 정책 문서	1095
자세히 알아보기	1095
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1095
이 정책 사용	1095
정책 세부 정보	1096
정책 버전	1096
JSON 정책 문서	1096
자세히 알아보기	1098
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1098
이 정책 사용	1099
정책 세부 정보	1099
정책 버전	1099
JSON 정책 문서	1099
자세히 알아보기	1109
AmazonSecurityLakeAdministrator	1109
이 정책 사용	1110
정책 세부 정보	1110
정책 버전	1110
JSON 정책 문서	1110
자세히 알아보기	1121
AmazonSecurityLakeMetastoreManager	1121
이 정책 사용	1122
정책 세부 정보	1122
정책 버전	1122
JSON 정책 문서	1122
자세히 알아보기	1124
AmazonSecurityLakePermissionsBoundary	1125
이 정책 사용	1125
정책 세부 정보	1125
정책 버전	1125
JSON 정책 문서	1125
자세히 알아보기	1128

AmazonSESEFullAccess	1129
이 정책 사용	1129
정책 세부 정보	1129
정책 버전	1129
JSON 정책 문서	1129
자세히 알아보기	1130
AmazonSESReadOnlyAccess	1130
이 정책 사용	1130
정책 세부 정보	1130
정책 버전	1130
JSON 정책 문서	1130
자세히 알아보기	1131
AmazonSESServiceRolePolicy	1131
이 정책 사용	1131
정책 세부 정보	1131
정책 버전	1132
JSON 정책 문서	1132
자세히 알아보기	1132
AmazonSNSFullAccess	1132
이 정책 사용	1133
정책 세부 정보	1133
정책 버전	1133
JSON 정책 문서	1133
자세히 알아보기	1133
AmazonSNSReadOnlyAccess	1134
이 정책 사용	1134
정책 세부 정보	1134
정책 버전	1134
JSON 정책 문서	1134
자세히 알아보기	1135
AmazonSNSRole	1135
이 정책 사용	1135
정책 세부 정보	1135
정책 버전	1135
JSON 정책 문서	1136
자세히 알아보기	1136

AmazonSQSFullAccess	1136
이 정책 사용	1136
정책 세부 정보	1137
정책 버전	1137
JSON 정책 문서	1137
자세히 알아보기	1137
AmazonSQSReadOnlyAccess	1138
이 정책 사용	1138
정책 세부 정보	1138
정책 버전	1138
JSON 정책 문서	1138
자세히 알아보기	1139
AmazonSSMAutomationApproverAccess	1139
이 정책 사용	1139
정책 세부 정보	1139
정책 버전	1139
JSON 정책 문서	1140
자세히 알아보기	1140
AmazonSSMAutomationRole	1140
이 정책 사용	1140
정책 세부 정보	1141
정책 버전	1141
JSON 정책 문서	1141
자세히 알아보기	1142
AmazonSSMDirectoryServiceAccess	1143
이 정책 사용	1143
정책 세부 정보	1143
정책 버전	1143
JSON 정책 문서	1143
자세히 알아보기	1144
AmazonSSMFullAccess	1144
이 정책 사용	1144
정책 세부 정보	1144
정책 버전	1144
JSON 정책 문서	1145
자세히 알아보기	1146

AmazonSSMMaintenanceWindowRole	1146
이 정책 사용	1146
정책 세부 정보	1146
정책 버전	1146
JSON 정책 문서	1147
자세히 알아보기	1148
AmazonSSMManagedEC2InstanceDefaultPolicy	1148
이 정책 사용	1148
정책 세부 정보	1149
정책 버전	1149
JSON 정책 문서	1149
자세히 알아보기	1150
AmazonSSMManagedInstanceCore	1150
이 정책 사용	1150
정책 세부 정보	1151
정책 버전	1151
JSON 정책 문서	1151
자세히 알아보기	1152
AmazonSSMPatchAssociation	1152
이 정책 사용	1153
정책 세부 정보	1153
정책 버전	1153
JSON 정책 문서	1153
자세히 알아보기	1154
AmazonSSMReadOnlyAccess	1154
이 정책 사용	1154
정책 세부 정보	1154
정책 버전	1154
JSON 정책 문서	1155
자세히 알아보기	1155
AmazonSSMServiceRolePolicy	1155
이 정책 사용	1155
정책 세부 정보	1155
정책 버전	1156
JSON 정책 문서	1156
자세히 알아보기	1161

AmazonSumerianFullAccess	1161
이 정책 사용	1161
정책 세부 정보	1161
정책 버전	1161
JSON 정책 문서	1162
자세히 알아보기	1162
AmazonTextractFullAccess	1162
이 정책 사용	1162
정책 세부 정보	1162
정책 버전	1163
JSON 정책 문서	1163
자세히 알아보기	1163
AmazonTextractServiceRole	1163
이 정책 사용	1164
정책 세부 정보	1164
정책 버전	1164
JSON 정책 문서	1164
자세히 알아보기	1164
AmazonTimestreamConsoleFullAccess	1165
이 정책 사용	1165
정책 세부 정보	1165
정책 버전	1165
JSON 정책 문서	1165
자세히 알아보기	1167
AmazonTimestreamFullAccess	1167
이 정책 사용	1167
정책 세부 정보	1168
정책 버전	1168
JSON 정책 문서	1168
자세히 알아보기	1169
AmazonTimestreamInfluxDBFullAccess	1169
이 정책 사용	1169
정책 세부 정보	1170
정책 버전	1170
JSON 정책 문서	1170
자세히 알아보기	1172

AmazonTimestreamInfluxDBServiceRolePolicy	1172
이 정책 사용	1172
정책 세부 정보	1172
정책 버전	1173
JSON 정책 문서	1173
자세히 알아보기	1175
AmazonTimestreamReadOnlyAccess	1175
이 정책 사용	1176
정책 세부 정보	1176
정책 버전	1176
JSON 정책 문서	1176
자세히 알아보기	1177
AmazonTranscribeFullAccess	1177
이 정책 사용	1177
정책 세부 정보	1177
정책 버전	1177
JSON 정책 문서	1178
자세히 알아보기	1178
AmazonTranscribeReadOnlyAccess	1178
이 정책 사용	1179
정책 세부 정보	1179
정책 버전	1179
JSON 정책 문서	1179
자세히 알아보기	1179
AmazonVPCCrossAccountNetworkInterfaceOperations	1180
이 정책 사용	1180
정책 세부 정보	1180
정책 버전	1180
JSON 정책 문서	1180
자세히 알아보기	1182
AmazonVPCFullAccess	1182
이 정책 사용	1182
정책 세부 정보	1182
정책 버전	1182
JSON 정책 문서	1183
자세히 알아보기	1186

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1187
이 정책 사용	1187
정책 세부 정보	1187
정책 버전	1187
JSON 정책 문서	1187
자세히 알아보기	1191
AmazonVPCReachabilityAnalyzerFullAccessPolicy	1191
이 정책 사용	1191
정책 세부 정보	1191
정책 버전	1191
JSON 정책 문서	1192
자세히 알아보기	1195
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1195
이 정책 사용	1195
정책 세부 정보	1195
정책 버전	1195
JSON 정책 문서	1196
자세히 알아보기	1196
AmazonVPCReadOnlyAccess	1196
이 정책 사용	1196
정책 세부 정보	1197
정책 버전	1197
JSON 정책 문서	1197
자세히 알아보기	1198
AmazonWorkDocsFullAccess	1198
이 정책 사용	1199
정책 세부 정보	1199
정책 버전	1199
JSON 정책 문서	1199
자세히 알아보기	1200
AmazonWorkDocsReadOnlyAccess	1200
이 정책 사용	1200
정책 세부 정보	1200
정책 버전	1200
JSON 정책 문서	1200
자세히 알아보기	1201

AmazonWorkMailEventsServiceRolePolicy	1201
이 정책 사용	1201
정책 세부 정보	1201
정책 버전	1202
JSON 정책 문서	1202
자세히 알아보기	1202
AmazonWorkMailFullAccess	1202
이 정책 사용	1203
정책 세부 정보	1203
정책 버전	1203
JSON 정책 문서	1203
자세히 알아보기	1205
AmazonWorkMailMessageFlowFullAccess	1205
이 정책 사용	1205
정책 세부 정보	1205
정책 버전	1206
JSON 정책 문서	1206
자세히 알아보기	1206
AmazonWorkMailMessageFlowReadOnlyAccess	1206
이 정책 사용	1207
정책 세부 정보	1207
정책 버전	1207
JSON 정책 문서	1207
자세히 알아보기	1207
AmazonWorkMailReadOnlyAccess	1208
이 정책 사용	1208
정책 세부 정보	1208
정책 버전	1208
JSON 정책 문서	1208
자세히 알아보기	1209
AmazonWorkSpacesAdmin	1209
이 정책 사용	1209
정책 세부 정보	1209
정책 버전	1210
JSON 정책 문서	1210
자세히 알아보기	1211

AmazonWorkSpacesApplicationManagerAdminAccess	1211
이 정책 사용	1211
정책 세부 정보	1211
정책 버전	1211
JSON 정책 문서	1212
자세히 알아보기	1212
AmazonWorkspacesPCAAccess	1212
이 정책 사용	1212
정책 세부 정보	1212
정책 버전	1213
JSON 정책 문서	1213
자세히 알아보기	1213
AmazonWorkSpacesSelfServiceAccess	1214
이 정책 사용	1214
정책 세부 정보	1214
정책 버전	1214
JSON 정책 문서	1214
자세히 알아보기	1215
AmazonWorkSpacesServiceAccess	1215
이 정책 사용	1215
정책 세부 정보	1215
정책 버전	1215
JSON 정책 문서	1216
자세히 알아보기	1216
AmazonWorkSpacesWebReadOnly	1216
이 정책 사용	1216
정책 세부 정보	1216
정책 버전	1217
JSON 정책 문서	1217
자세히 알아보기	1218
AmazonWorkSpacesWebServiceRolePolicy	1218
이 정책 사용	1218
정책 세부 정보	1218
정책 버전	1219
JSON 정책 문서	1219
자세히 알아보기	1221

AmazonZocaloFullAccess	1221
이 정책 사용	1221
정책 세부 정보	1221
정책 버전	1222
JSON 정책 문서	1222
자세히 알아보기	1222
AmazonZocaloReadOnlyAccess	1223
이 정책 사용	1223
정책 세부 정보	1223
정책 버전	1223
JSON 정책 문서	1223
자세히 알아보기	1224
AmplifyBackendDeployFullAccess	1224
이 정책 사용	1224
정책 세부 정보	1224
정책 버전	1224
JSON 정책 문서	1225
자세히 알아보기	1228
APIGatewayServiceRolePolicy	1229
이 정책 사용	1229
정책 세부 정보	1229
정책 버전	1229
JSON 정책 문서	1229
자세히 알아보기	1232
AppIntegrationsServiceLinkedRolePolicy	1232
이 정책 사용	1232
정책 세부 정보	1232
정책 버전	1232
JSON 정책 문서	1232
자세히 알아보기	1234
ApplicationAutoScalingForAmazonAppStreamAccess	1234
이 정책 사용	1234
정책 세부 정보	1234
정책 버전	1235
JSON 정책 문서	1235
자세히 알아보기	1235

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1236
이 정책 사용	1236
정책 세부 정보	1236
정책 버전	1236
JSON 정책 문서	1236
자세히 알아보기	1238
AppRunnerNetworkingServiceRolePolicy	1239
이 정책 사용	1239
정책 세부 정보	1239
정책 버전	1239
JSON 정책 문서	1239
자세히 알아보기	1241
AppRunnerServiceRolePolicy	1241
이 정책 사용	1241
정책 세부 정보	1241
정책 버전	1241
JSON 정책 문서	1241
자세히 알아보기	1242
AutoScalingConsoleFullAccess	1242
이 정책 사용	1243
정책 세부 정보	1243
정책 버전	1243
JSON 정책 문서	1243
자세히 알아보기	1245
AutoScalingConsoleReadOnlyAccess	1245
이 정책 사용	1245
정책 세부 정보	1245
정책 버전	1245
JSON 정책 문서	1246
자세히 알아보기	1247
AutoScalingFullAccess	1247
이 정책 사용	1247
정책 세부 정보	1247
정책 버전	1247
JSON 정책 문서	1248
자세히 알아보기	1249

AutoScalingNotificationAccessRole	1249
이 정책 사용	1249
정책 세부 정보	1249
정책 버전	1250
JSON 정책 문서	1250
자세히 알아보기	1250
AutoScalingReadOnlyAccess	1250
이 정책 사용	1251
정책 세부 정보	1251
정책 버전	1251
JSON 정책 문서	1251
자세히 알아보기	1251
AutoScalingServiceRolePolicy	1252
이 정책 사용	1252
정책 세부 정보	1252
정책 버전	1252
JSON 정책 문서	1252
자세히 알아보기	1255
AWS_ConfigRole	1255
이 정책 사용	1255
정책 세부 정보	1255
정책 버전	1256
JSON 정책 문서	1256
자세히 알아보기	1287
AWSAccountActivityAccess	1287
이 정책 사용	1287
정책 세부 정보	1287
정책 버전	1287
JSON 정책 문서	1287
자세히 알아보기	1288
AWSAccountManagementFullAccess	1288
이 정책 사용	1289
정책 세부 정보	1289
정책 버전	1289
JSON 정책 문서	1289
자세히 알아보기	1289

AWSAccountManagementReadOnlyAccess	1290
이 정책 사용	1290
정책 세부 정보	1290
정책 버전	1290
JSON 정책 문서	1290
자세히 알아보기	1291
AWSAccountUsageReportAccess	1291
이 정책 사용	1291
정책 세부 정보	1291
정책 버전	1291
JSON 정책 문서	1291
자세히 알아보기	1292
AWSAgentlessDiscoveryService	1292
이 정책 사용	1292
정책 세부 정보	1292
정책 버전	1292
JSON 정책 문서	1293
자세히 알아보기	1294
AWSAppFabricFullAccess	1295
이 정책 사용	1295
정책 세부 정보	1295
정책 버전	1295
JSON 정책 문서	1295
자세히 알아보기	1297
AWSAppFabricReadOnlyAccess	1297
이 정책 사용	1297
정책 세부 정보	1297
정책 버전	1297
JSON 정책 문서	1297
자세히 알아보기	1298
AWSAppFabricServiceRolePolicy	1298
이 정책 사용	1298
정책 세부 정보	1299
정책 버전	1299
JSON 정책 문서	1299
자세히 알아보기	1300

AWSApplicationAutoscalingAppStreamFleetPolicy	1300
이 정책 사용	1300
정책 세부 정보	1301
정책 버전	1301
JSON 정책 문서	1301
자세히 알아보기	1302
AWSApplicationAutoscalingCassandraTablePolicy	1302
이 정책 사용	1302
정책 세부 정보	1302
정책 버전	1302
JSON 정책 문서	1302
자세히 알아보기	1303
AWSApplicationAutoscalingComprehendEndpointPolicy	1303
이 정책 사용	1303
정책 세부 정보	1303
정책 버전	1304
JSON 정책 문서	1304
자세히 알아보기	1304
AWSApplicationAutoScalingCustomResourcePolicy	1305
이 정책 사용	1305
정책 세부 정보	1305
정책 버전	1305
JSON 정책 문서	1305
자세히 알아보기	1306
AWSApplicationAutoscalingDynamoDBTablePolicy	1306
이 정책 사용	1306
정책 세부 정보	1306
정책 버전	1306
JSON 정책 문서	1307
자세히 알아보기	1307
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1307
이 정책 사용	1307
정책 세부 정보	1308
정책 버전	1308
JSON 정책 문서	1308
자세히 알아보기	1309

AWSApplicationAutoscalingECSServicePolicy	1309
이 정책 사용	1309
정책 세부 정보	1309
정책 버전	1309
JSON 정책 문서	1309
자세히 알아보기	1310
AWSApplicationAutoscalingElastiCacheRGPolicy	1310
이 정책 사용	1310
정책 세부 정보	1310
정책 버전	1311
JSON 정책 문서	1311
자세히 알아보기	1312
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1312
이 정책 사용	1312
정책 세부 정보	1312
정책 버전	1312
JSON 정책 문서	1313
자세히 알아보기	1313
AWSApplicationAutoscalingKafkaClusterPolicy	1313
이 정책 사용	1313
정책 세부 정보	1313
정책 버전	1314
JSON 정책 문서	1314
자세히 알아보기	1314
AWSApplicationAutoscalingLambdaConcurrencyPolicy	1315
이 정책 사용	1315
정책 세부 정보	1315
정책 버전	1315
JSON 정책 문서	1315
자세히 알아보기	1316
AWSApplicationAutoscalingNeptuneClusterPolicy	1316
이 정책 사용	1316
정책 세부 정보	1316
정책 버전	1316
JSON 정책 문서	1317
자세히 알아보기	1318

AWSApplicationAutoscalingRDSClusterPolicy	1318
이 정책 사용	1318
정책 세부 정보	1319
정책 버전	1319
JSON 정책 문서	1319
자세히 알아보기	1320
AWSApplicationAutoscalingSageMakerEndpointPolicy	1320
이 정책 사용	1320
정책 세부 정보	1320
정책 버전	1320
JSON 정책 문서	1321
자세히 알아보기	1321
AWSApplicationDiscoveryAgentAccess	1322
이 정책 사용	1322
정책 세부 정보	1322
정책 버전	1322
JSON 정책 문서	1322
자세히 알아보기	1323
AWSApplicationDiscoveryAgentlessCollectorAccess	1323
이 정책 사용	1323
정책 세부 정보	1323
정책 버전	1324
JSON 정책 문서	1324
자세히 알아보기	1325
AWSApplicationDiscoveryServiceFullAccess	1325
이 정책 사용	1325
정책 세부 정보	1325
정책 버전	1326
JSON 정책 문서	1326
자세히 알아보기	1327
AWSApplicationMigrationAgentInstallationPolicy	1327
이 정책 사용	1328
정책 세부 정보	1328
정책 버전	1328
JSON 정책 문서	1328
자세히 알아보기	1329

AWSApplicationMigrationAgentPolicy	1329
이 정책 사용	1329
정책 세부 정보	1329
정책 버전	1330
JSON 정책 문서	1330
자세히 알아보기	1331
AWSApplicationMigrationAgentPolicy_v2	1331
이 정책 사용	1331
정책 세부 정보	1331
정책 버전	1332
JSON 정책 문서	1332
자세히 알아보기	1332
AWSApplicationMigrationConversionServerPolicy	1333
이 정책 사용	1333
정책 세부 정보	1333
정책 버전	1333
JSON 정책 문서	1333
자세히 알아보기	1334
AWSApplicationMigrationEC2Access	1334
이 정책 사용	1334
정책 세부 정보	1334
정책 버전	1335
JSON 정책 문서	1335
자세히 알아보기	1342
AWSApplicationMigrationFullAccess	1343
이 정책 사용	1343
정책 세부 정보	1343
정책 버전	1343
JSON 정책 문서	1343
자세히 알아보기	1349
AWSApplicationMigrationMGHAccess	1349
이 정책 사용	1350
정책 세부 정보	1350
정책 버전	1350
JSON 정책 문서	1350
자세히 알아보기	1351

AWSApplicationMigrationReadOnlyAccess	1351
이 정책 사용	1351
정책 세부 정보	1351
정책 버전	1351
JSON 정책 문서	1352
자세히 알아보기	1353
AWSApplicationMigrationReplicationServerPolicy	1353
이 정책 사용	1353
정책 세부 정보	1353
정책 버전	1354
JSON 정책 문서	1354
자세히 알아보기	1355
AWSApplicationMigrationServiceEc2InstancePolicy	1356
이 정책 사용	1356
정책 세부 정보	1356
정책 버전	1356
JSON 정책 문서	1356
자세히 알아보기	1358
AWSApplicationMigrationServiceRolePolicy	1358
이 정책 사용	1358
정책 세부 정보	1358
정책 버전	1358
JSON 정책 문서	1359
자세히 알아보기	1366
AWSApplicationMigrationSSMAccess	1366
이 정책 사용	1366
정책 세부 정보	1366
정책 버전	1366
JSON 정책 문서	1366
자세히 알아보기	1368
AWSApplicationMigrationVCenterClientPolicy	1369
이 정책 사용	1369
정책 세부 정보	1369
정책 버전	1369
JSON 정책 문서	1369
자세히 알아보기	1370

AWSAppMeshEnvoyAccess	1370
이 정책 사용	1370
정책 세부 정보	1370
정책 버전	1371
JSON 정책 문서	1371
자세히 알아보기	1371
AWSAppMeshFullAccess	1371
이 정책 사용	1372
정책 세부 정보	1372
정책 버전	1372
JSON 정책 문서	1372
자세히 알아보기	1373
AWSAppMeshPreviewEnvoyAccess	1374
이 정책 사용	1374
정책 세부 정보	1374
정책 버전	1374
JSON 정책 문서	1374
자세히 알아보기	1375
AWSAppMeshPreviewServiceRolePolicy	1375
이 정책 사용	1375
정책 세부 정보	1375
정책 버전	1375
JSON 정책 문서	1376
자세히 알아보기	1376
AWSAppMeshReadOnly	1376
이 정책 사용	1377
정책 세부 정보	1377
정책 버전	1377
JSON 정책 문서	1377
자세히 알아보기	1378
AWSAppMeshServiceRolePolicy	1378
이 정책 사용	1378
정책 세부 정보	1379
정책 버전	1379
JSON 정책 문서	1379
자세히 알아보기	1380

AWSAppRunnerFullAccess	1380
이 정책 사용	1380
정책 세부 정보	1380
정책 버전	1380
JSON 정책 문서	1380
자세히 알아보기	1381
AWSAppRunnerReadOnlyAccess	1381
이 정책 사용	1382
정책 세부 정보	1382
정책 버전	1382
JSON 정책 문서	1382
자세히 알아보기	1382
AWSAppRunnerServicePolicyForECRAccess	1383
이 정책 사용	1383
정책 세부 정보	1383
정책 버전	1383
JSON 정책 문서	1383
자세히 알아보기	1384
AWSAppSyncAdministrator	1384
이 정책 사용	1384
정책 세부 정보	1384
정책 버전	1385
JSON 정책 문서	1385
자세히 알아보기	1386
AWSAppSyncInvokeFullAccess	1386
이 정책 사용	1386
정책 세부 정보	1386
정책 버전	1387
JSON 정책 문서	1387
자세히 알아보기	1387
AWSAppSyncPushToCloudWatchLogs	1387
이 정책 사용	1388
정책 세부 정보	1388
정책 버전	1388
JSON 정책 문서	1388
자세히 알아보기	1388

AWSAppSyncSchemaAuthor	1389
이 정책 사용	1389
정책 세부 정보	1389
정책 버전	1389
JSON 정책 문서	1389
자세히 알아보기	1390
AWSAppSyncServiceRolePolicy	1391
이 정책 사용	1391
정책 세부 정보	1391
정책 버전	1391
JSON 정책 문서	1391
자세히 알아보기	1392
AWSArtifactAccountSync	1392
이 정책 사용	1392
정책 세부 정보	1392
정책 버전	1392
JSON 정책 문서	1393
자세히 알아보기	1393
AWSArtifactReportsReadOnlyAccess	1393
이 정책 사용	1393
정책 세부 정보	1393
정책 버전	1394
JSON 정책 문서	1394
자세히 알아보기	1394
AWSArtifactServiceRolePolicy	1395
이 정책 사용	1395
정책 세부 정보	1395
정책 버전	1395
JSON 정책 문서	1395
자세히 알아보기	1396
AWSAuditManagerAdministratorAccess	1396
이 정책 사용	1396
정책 세부 정보	1396
정책 버전	1396
JSON 정책 문서	1397
자세히 알아보기	1401

AWSAuditManagerServiceRolePolicy	1401
이 정책 사용	1401
정책 세부 정보	1401
정책 버전	1401
JSON 정책 문서	1402
자세히 알아보기	1408
AWSAutoScalingPlansEC2AutoScalingPolicy	1408
이 정책 사용	1409
정책 세부 정보	1409
정책 버전	1409
JSON 정책 문서	1409
자세히 알아보기	1410
AWSBackupAuditAccess	1410
이 정책 사용	1410
정책 세부 정보	1410
정책 버전	1410
JSON 정책 문서	1410
자세히 알아보기	1412
AWSBackupDataTransferAccess	1412
이 정책 사용	1412
정책 세부 정보	1412
정책 버전	1412
JSON 정책 문서	1413
자세히 알아보기	1413
AWSBackupFullAccess	1413
이 정책 사용	1414
정책 세부 정보	1414
정책 버전	1414
JSON 정책 문서	1414
자세히 알아보기	1424
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	1424
이 정책 사용	1424
정책 세부 정보	1424
정책 버전	1425
JSON 정책 문서	1425
자세히 알아보기	1425

AWSBackupOperatorAccess	1426
이 정책 사용	1426
정책 세부 정보	1426
정책 버전	1426
JSON 정책 문서	1426
자세히 알아보기	1433
AWSBackupOrganizationAdminAccess	1433
이 정책 사용	1433
정책 세부 정보	1433
정책 버전	1434
JSON 정책 문서	1434
자세히 알아보기	1436
AWSBackupRestoreAccessForSAPHANA	1436
이 정책 사용	1436
정책 세부 정보	1436
정책 버전	1436
JSON 정책 문서	1437
자세히 알아보기	1437
AWSBackupServiceLinkedRolePolicyForBackup	1438
이 정책 사용	1438
정책 세부 정보	1438
정책 버전	1438
JSON 정책 문서	1438
자세히 알아보기	1446
AWSBackupServiceLinkedRolePolicyForBackupTest	1446
이 정책 사용	1447
정책 세부 정보	1447
정책 버전	1447
JSON 정책 문서	1447
자세히 알아보기	1448
AWSBackupServiceRolePolicyForBackup	1448
이 정책 사용	1448
정책 세부 정보	1448
정책 버전	1448
JSON 정책 문서	1449
자세히 알아보기	1460

AWSBackupServiceRolePolicyForRestores	1460
이 정책 사용	1460
정책 세부 정보	1460
정책 버전	1460
JSON 정책 문서	1461
자세히 알아보기	1470
AWSBackupServiceRolePolicyForS3Backup	1471
이 정책 사용	1471
정책 세부 정보	1471
정책 버전	1471
JSON 정책 문서	1471
자세히 알아보기	1474
AWSBackupServiceRolePolicyForS3Restore	1474
이 정책 사용	1474
정책 세부 정보	1474
정책 버전	1474
JSON 정책 문서	1474
자세히 알아보기	1476
AWSBatchFullAccess	1476
이 정책 사용	1476
정책 세부 정보	1476
정책 버전	1476
JSON 정책 문서	1477
자세히 알아보기	1478
AWSBatchServiceEventTargetRole	1478
이 정책 사용	1478
정책 세부 정보	1479
정책 버전	1479
JSON 정책 문서	1479
자세히 알아보기	1479
AWSBatchServiceRole	1480
이 정책 사용	1480
정책 세부 정보	1480
정책 버전	1480
JSON 정책 문서	1480
자세히 알아보기	1483

AWSBCMDDataExportsServiceRolePolicy	1484
이 정책 사용	1484
정책 세부 정보	1484
정책 버전	1484
JSON 정책 문서	1484
자세히 알아보기	1485
AWSBillingConductorFullAccess	1485
이 정책 사용	1485
정책 세부 정보	1485
정책 버전	1485
JSON 정책 문서	1486
자세히 알아보기	1486
AWSBillingConductorReadOnlyAccess	1486
이 정책 사용	1486
정책 세부 정보	1486
정책 버전	1487
JSON 정책 문서	1487
자세히 알아보기	1487
AWSBillingReadOnlyAccess	1488
이 정책 사용	1488
정책 세부 정보	1488
정책 버전	1488
JSON 정책 문서	1488
자세히 알아보기	1490
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	1490
이 정책 사용	1490
정책 세부 정보	1490
정책 버전	1490
JSON 정책 문서	1491
자세히 알아보기	1492
AWSBudgetsActionsWithAWSResourceControlAccess	1492
이 정책 사용	1492
정책 세부 정보	1492
정책 버전	1492
JSON 정책 문서	1493
자세히 알아보기	1494

AWSBudgetsReadOnlyAccess	1494
이 정책 사용	1494
정책 세부 정보	1494
정책 버전	1494
JSON 정책 문서	1495
자세히 알아보기	1495
AWSBugBustFullAccess	1495
이 정책 사용	1495
정책 세부 정보	1496
정책 버전	1496
JSON 정책 문서	1496
자세히 알아보기	1497
AWSBugBustPlayerAccess	1497
이 정책 사용	1497
정책 세부 정보	1498
정책 버전	1498
JSON 정책 문서	1498
자세히 알아보기	1499
AWSBugBustServiceRolePolicy	1499
이 정책 사용	1499
정책 세부 정보	1499
정책 버전	1500
JSON 정책 문서	1500
자세히 알아보기	1500
AWSCertificateManagerFullAccess	1501
이 정책 사용	1501
정책 세부 정보	1501
정책 버전	1501
JSON 정책 문서	1501
자세히 알아보기	1502
AWSCertificateManagerPrivateCAAuditor	1502
이 정책 사용	1502
정책 세부 정보	1503
정책 버전	1503
JSON 정책 문서	1503
자세히 알아보기	1504

AWSCertificateManagerPrivateCAFullAccess	1504
이 정책 사용	1504
정책 세부 정보	1504
정책 버전	1504
JSON 정책 문서	1505
자세히 알아보기	1505
AWSCertificateManagerPrivateCAPrivilegedUser	1505
이 정책 사용	1505
정책 세부 정보	1505
정책 버전	1506
JSON 정책 문서	1506
자세히 알아보기	1507
AWSCertificateManagerPrivateCAReadOnly	1507
이 정책 사용	1507
정책 세부 정보	1507
정책 버전	1508
JSON 정책 문서	1508
자세히 알아보기	1508
AWSCertificateManagerPrivateCAUser	1509
이 정책 사용	1509
정책 세부 정보	1509
정책 버전	1509
JSON 정책 문서	1509
자세히 알아보기	1510
AWSCertificateManagerReadOnly	1511
이 정책 사용	1511
정책 세부 정보	1511
정책 버전	1511
JSON 정책 문서	1511
자세히 알아보기	1512
AWSChatbotServiceLinkedRolePolicy	1512
이 정책 사용	1512
정책 세부 정보	1512
정책 버전	1512
JSON 정책 문서	1513
자세히 알아보기	1513

AWSCleanRoomsFullAccess	1514
이 정책 사용	1514
정책 세부 정보	1514
정책 버전	1514
JSON 정책 문서	1514
자세히 알아보기	1519
AWSCleanRoomsFullAccessNoQuerying	1519
이 정책 사용	1519
정책 세부 정보	1519
정책 버전	1519
JSON 정책 문서	1520
자세히 알아보기	1524
AWSCleanRoomsMLFullAccess	1525
이 정책 사용	1525
정책 세부 정보	1525
정책 버전	1525
JSON 정책 문서	1525
자세히 알아보기	1529
AWSCleanRoomsMLReadOnlyAccess	1529
이 정책 사용	1529
정책 세부 정보	1529
정책 버전	1529
JSON 정책 문서	1530
자세히 알아보기	1531
AWSCleanRoomsReadOnlyAccess	1531
이 정책 사용	1531
정책 세부 정보	1531
정책 버전	1531
JSON 정책 문서	1531
자세히 알아보기	1533
AWSCloud9Administrator	1533
이 정책 사용	1533
정책 세부 정보	1533
정책 버전	1533
JSON 정책 문서	1533
자세히 알아보기	1535

AWSCloud9EnvironmentMember	1535
이 정책 사용	1535
정책 세부 정보	1535
정책 버전	1535
JSON 정책 문서	1536
자세히 알아보기	1537
AWSCloud9ServiceRolePolicy	1537
이 정책 사용	1537
정책 세부 정보	1537
정책 버전	1538
JSON 정책 문서	1538
자세히 알아보기	1540
AWSCloud9SSMInstanceProfile	1540
이 정책 사용	1541
정책 세부 정보	1541
정책 버전	1541
JSON 정책 문서	1541
자세히 알아보기	1542
AWSCloud9User	1542
이 정책 사용	1542
정책 세부 정보	1542
정책 버전	1542
JSON 정책 문서	1542
자세히 알아보기	1545
AWSCloudFormationFullAccess	1545
이 정책 사용	1545
정책 세부 정보	1545
정책 버전	1545
JSON 정책 문서	1546
자세히 알아보기	1546
AWSCloudFormationReadOnlyAccess	1546
이 정책 사용	1546
정책 세부 정보	1546
정책 버전	1547
JSON 정책 문서	1547
자세히 알아보기	1547

AWSCloudFrontLogger	1547
이 정책 사용	1548
정책 세부 정보	1548
정책 버전	1548
JSON 정책 문서	1548
자세히 알아보기	1549
AWSCloudHSMFullAccess	1549
이 정책 사용	1549
정책 세부 정보	1549
정책 버전	1549
JSON 정책 문서	1549
자세히 알아보기	1550
AWSCloudHSMReadOnlyAccess	1550
이 정책 사용	1550
정책 세부 정보	1550
정책 버전	1550
JSON 정책 문서	1551
자세히 알아보기	1551
AWSCloudHSMRole	1551
이 정책 사용	1551
정책 세부 정보	1551
정책 버전	1552
JSON 정책 문서	1552
자세히 알아보기	1552
AWSCloudMapDiscoverInstanceAccess	1553
이 정책 사용	1553
정책 세부 정보	1553
정책 버전	1553
JSON 정책 문서	1553
자세히 알아보기	1554
AWSCloudMapFullAccess	1554
이 정책 사용	1554
정책 세부 정보	1554
정책 버전	1554
JSON 정책 문서	1555
자세히 알아보기	1555

AWSCloudMapReadOnlyAccess	1555
이 정책 사용	1556
정책 세부 정보	1556
정책 버전	1556
JSON 정책 문서	1556
자세히 알아보기	1557
AWSCloudMapRegisterInstanceAccess	1557
이 정책 사용	1557
정책 세부 정보	1557
정책 버전	1557
JSON 정책 문서	1557
자세히 알아보기	1558
AWSCloudShellFullAccess	1558
이 정책 사용	1558
정책 세부 정보	1559
정책 버전	1559
JSON 정책 문서	1559
자세히 알아보기	1559
AWSCloudTrail_FullAccess	1560
이 정책 사용	1560
정책 세부 정보	1560
정책 버전	1560
JSON 정책 문서	1560
자세히 알아보기	1563
AWSCloudTrail_ReadOnlyAccess	1563
이 정책 사용	1563
정책 세부 정보	1563
정책 버전	1563
JSON 정책 문서	1564
자세히 알아보기	1564
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	1564
이 정책 사용	1564
정책 세부 정보	1565
정책 버전	1565
JSON 정책 문서	1565
자세히 알아보기	1565

AWSCodeArtifactAdminAccess	1565
이 정책 사용	1566
정책 세부 정보	1566
정책 버전	1566
JSON 정책 문서	1566
자세히 알아보기	1567
AWSCodeArtifactReadOnlyAccess	1567
이 정책 사용	1567
정책 세부 정보	1567
정책 버전	1567
JSON 정책 문서	1568
자세히 알아보기	1568
AWSCodeBuildAdminAccess	1569
이 정책 사용	1569
정책 세부 정보	1569
정책 버전	1569
JSON 정책 문서	1569
자세히 알아보기	1573
AWSCodeBuildDeveloperAccess	1573
이 정책 사용	1573
정책 세부 정보	1573
정책 버전	1573
JSON 정책 문서	1573
자세히 알아보기	1576
AWSCodeBuildReadOnlyAccess	1576
이 정책 사용	1576
정책 세부 정보	1577
정책 버전	1577
JSON 정책 문서	1577
자세히 알아보기	1578
AWSCodeCommitFullAccess	1579
이 정책 사용	1579
정책 세부 정보	1579
정책 버전	1579
JSON 정책 문서	1579
자세히 알아보기	1584

AWSCodeCommitPowerUser	1584
이 정책 사용	1584
정책 세부 정보	1584
정책 버전	1585
JSON 정책 문서	1585
자세히 알아보기	1589
AWSCodeCommitReadOnly	1590
이 정책 사용	1590
정책 세부 정보	1590
정책 버전	1590
JSON 정책 문서	1590
자세히 알아보기	1593
AWSCodeDeployDeployerAccess	1593
이 정책 사용	1593
정책 세부 정보	1593
정책 버전	1594
JSON 정책 문서	1594
자세히 알아보기	1595
AWSCodeDeployFullAccess	1595
이 정책 사용	1596
정책 세부 정보	1596
정책 버전	1596
JSON 정책 문서	1596
자세히 알아보기	1598
AWSCodeDeployReadOnlyAccess	1598
이 정책 사용	1598
정책 세부 정보	1598
정책 버전	1598
JSON 정책 문서	1598
자세히 알아보기	1599
AWSCodeDeployRole	1600
이 정책 사용	1600
정책 세부 정보	1600
정책 버전	1600
JSON 정책 문서	1600
자세히 알아보기	1602

AWSCodeDeployRoleForCloudFormation	1602
이 정책 사용	1602
정책 세부 정보	1602
정책 버전	1602
JSON 정책 문서	1602
자세히 알아보기	1603
AWSCodeDeployRoleForECS	1603
이 정책 사용	1603
정책 세부 정보	1603
정책 버전	1604
JSON 정책 문서	1604
자세히 알아보기	1605
AWSCodeDeployRoleForECSLimited	1605
이 정책 사용	1605
정책 세부 정보	1605
정책 버전	1605
JSON 정책 문서	1606
자세히 알아보기	1607
AWSCodeDeployRoleForLambda	1608
이 정책 사용	1608
정책 세부 정보	1608
정책 버전	1608
JSON 정책 문서	1608
자세히 알아보기	1609
AWSCodeDeployRoleForLambdaLimited	1610
이 정책 사용	1610
정책 세부 정보	1610
정책 버전	1610
JSON 정책 문서	1610
자세히 알아보기	1611
AWSCodePipeline_FullAccess	1612
이 정책 사용	1612
정책 세부 정보	1612
정책 버전	1612
JSON 정책 문서	1612
자세히 알아보기	1616

AWSCodePipeline_ReadOnlyAccess	1616
이 정책 사용	1616
정책 세부 정보	1616
정책 버전	1617
JSON 정책 문서	1617
자세히 알아보기	1618
AWSCodePipelineApproverAccess	1618
이 정책 사용	1618
정책 세부 정보	1618
정책 버전	1619
JSON 정책 문서	1619
자세히 알아보기	1619
AWSCodePipelineCustomActionAccess	1619
이 정책 사용	1620
정책 세부 정보	1620
정책 버전	1620
JSON 정책 문서	1620
자세히 알아보기	1621
AWSCodeStarFullAccess	1621
이 정책 사용	1621
정책 세부 정보	1621
정책 버전	1621
JSON 정책 문서	1621
자세히 알아보기	1622
AWSCodeStarNotificationsServiceRolePolicy	1622
이 정책 사용	1623
정책 세부 정보	1623
정책 버전	1623
JSON 정책 문서	1623
자세히 알아보기	1624
AWSCodeStarServiceRole	1624
이 정책 사용	1625
정책 세부 정보	1625
정책 버전	1625
JSON 정책 문서	1625
자세히 알아보기	1630

AWSCompromisedKeyQuarantine	1630
이 정책 사용	1630
정책 세부 정보	1630
정책 버전	1631
JSON 정책 문서	1631
자세히 알아보기	1632
AWSCompromisedKeyQuarantineV2	1632
이 정책 사용	1632
정책 세부 정보	1632
정책 버전	1632
JSON 정책 문서	1633
자세히 알아보기	1634
AWSConfigMultiAccountSetupPolicy	1635
이 정책 사용	1635
정책 세부 정보	1635
정책 버전	1635
JSON 정책 문서	1635
자세히 알아보기	1637
AWSConfigRemediationServiceRolePolicy	1637
이 정책 사용	1638
정책 세부 정보	1638
정책 버전	1638
JSON 정책 문서	1638
자세히 알아보기	1639
AWSConfigRoleForOrganizations	1639
이 정책 사용	1639
정책 세부 정보	1639
정책 버전	1639
JSON 정책 문서	1640
자세히 알아보기	1640
AWSConfigRulesExecutionRole	1640
이 정책 사용	1640
정책 세부 정보	1641
정책 버전	1641
JSON 정책 문서	1641
자세히 알아보기	1642

AWSConfigServiceRolePolicy	1642
이 정책 사용	1642
정책 세부 정보	1642
정책 버전	1642
JSON 정책 문서	1643
자세히 알아보기	1674
AWSConfigUserAccess	1674
이 정책 사용	1674
정책 세부 정보	1674
정책 버전	1675
JSON 정책 문서	1675
자세히 알아보기	1675
AWSConnector	1676
이 정책 사용	1676
정책 세부 정보	1676
정책 버전	1676
JSON 정책 문서	1676
자세히 알아보기	1678
AWSControlTowerAccountServiceRolePolicy	1678
이 정책 사용	1679
정책 세부 정보	1679
정책 버전	1679
JSON 정책 문서	1679
자세히 알아보기	1681
AWSControlTowerServiceRolePolicy	1681
이 정책 사용	1681
정책 세부 정보	1681
정책 버전	1681
JSON 정책 문서	1682
자세히 알아보기	1686
AWSCostAndUsageReportAutomationPolicy	1686
이 정책 사용	1686
정책 세부 정보	1687
정책 버전	1687
JSON 정책 문서	1687
자세히 알아보기	1688

AWSDataExchangeFullAccess	1688
이 정책 사용	1688
정책 세부 정보	1688
정책 버전	1689
JSON 정책 문서	1689
자세히 알아보기	1692
AWSDataExchangeProviderFullAccess	1693
이 정책 사용	1693
정책 세부 정보	1693
정책 버전	1693
JSON 정책 문서	1693
자세히 알아보기	1697
AWSDataExchangeReadOnly	1697
이 정책 사용	1697
정책 세부 정보	1697
정책 버전	1697
JSON 정책 문서	1698
자세히 알아보기	1698
AWSDataExchangeSubscriberFullAccess	1699
이 정책 사용	1699
정책 세부 정보	1699
정책 버전	1699
JSON 정책 문서	1699
자세히 알아보기	1702
AWSDataLifecycleManagerServiceRole	1702
이 정책 사용	1702
정책 세부 정보	1702
정책 버전	1702
JSON 정책 문서	1702
자세히 알아보기	1704
AWSDataLifecycleManagerServiceRoleForAMIManagement	1704
이 정책 사용	1704
정책 세부 정보	1704
정책 버전	1704
JSON 정책 문서	1705
자세히 알아보기	1706

AWSDatalifecycleManagerSSMFullAccess	1706
이 정책 사용	1706
정책 세부 정보	1706
정책 버전	1706
JSON 정책 문서	1707
자세히 알아보기	1708
AWSDatapipeline_FullAccess	1708
이 정책 사용	1708
정책 세부 정보	1708
정책 버전	1709
JSON 정책 문서	1709
자세히 알아보기	1710
AWSDatapipeline_PowerUser	1710
이 정책 사용	1710
정책 세부 정보	1710
정책 버전	1710
JSON 정책 문서	1711
자세히 알아보기	1712
AWSDatasyncDiscoveryServiceRolePolicy	1712
이 정책 사용	1712
정책 세부 정보	1712
정책 버전	1712
JSON 정책 문서	1712
자세히 알아보기	1713
AWSDatasyncFullAccess	1714
이 정책 사용	1714
정책 세부 정보	1714
정책 버전	1714
JSON 정책 문서	1714
자세히 알아보기	1716
AWSDatasyncReadOnlyAccess	1716
이 정책 사용	1716
정책 세부 정보	1716
정책 버전	1716
JSON 정책 문서	1716
자세히 알아보기	1717

AWSDeadlineCloud-FleetWorker	1717
이 정책 사용	1717
정책 세부 정보	1718
정책 버전	1718
JSON 정책 문서	1718
자세히 알아보기	1719
AWSDeadlineCloud-UserAccessFarms	1719
이 정책 사용	1719
정책 세부 정보	1719
정책 버전	1719
JSON 정책 문서	1719
자세히 알아보기	1725
AWSDeadlineCloud-UserAccessFleets	1725
이 정책 사용	1725
정책 세부 정보	1725
정책 버전	1725
JSON 정책 문서	1726
자세히 알아보기	1729
AWSDeadlineCloud-UserAccessJobs	1729
이 정책 사용	1730
정책 세부 정보	1730
정책 버전	1730
JSON 정책 문서	1730
자세히 알아보기	1734
AWSDeadlineCloud-UserAccessQueues	1734
이 정책 사용	1734
정책 세부 정보	1734
정책 버전	1735
JSON 정책 문서	1735
자세히 알아보기	1739
AWSDeadlineCloud-WorkerHost	1740
이 정책 사용	1740
정책 세부 정보	1740
정책 버전	1740
JSON 정책 문서	1740
자세히 알아보기	1741

AWSDeepLensLambdaFunctionAccessPolicy	1741
이 정책 사용	1741
정책 세부 정보	1741
정책 버전	1741
JSON 정책 문서	1742
자세히 알아보기	1743
AWSDeepLensServiceRolePolicy	1743
이 정책 사용	1743
정책 세부 정보	1743
정책 버전	1744
JSON 정책 문서	1744
자세히 알아보기	1751
AWSDeepRacerAccountAdminAccess	1751
이 정책 사용	1751
정책 세부 정보	1751
정책 버전	1751
JSON 정책 문서	1752
자세히 알아보기	1752
AWSDeepRacerCloudFormationAccessPolicy	1752
이 정책 사용	1753
정책 세부 정보	1753
정책 버전	1753
JSON 정책 문서	1753
자세히 알아보기	1756
AWSDeepRacerDefaultMultiUserAccess	1756
이 정책 사용	1756
정책 세부 정보	1756
정책 버전	1757
JSON 정책 문서	1757
자세히 알아보기	1758
AWSDeepRacerFullAccess	1758
이 정책 사용	1759
정책 세부 정보	1759
정책 버전	1759
JSON 정책 문서	1759
자세히 알아보기	1760

AWSDeepRacerRoboMakerAccessPolicy	1760
이 정책 사용	1760
정책 세부 정보	1761
정책 버전	1761
JSON 정책 문서	1761
자세히 알아보기	1763
AWSDeepRacerServiceRolePolicy	1763
이 정책 사용	1763
정책 세부 정보	1763
정책 버전	1764
JSON 정책 문서	1764
자세히 알아보기	1767
AWSDenyAll	1767
이 정책 사용	1767
정책 세부 정보	1767
정책 버전	1767
JSON 정책 문서	1768
자세히 알아보기	1768
AWSDeviceFarmFullAccess	1768
이 정책 사용	1768
정책 세부 정보	1769
정책 버전	1769
JSON 정책 문서	1769
자세히 알아보기	1769
AWSDeviceFarmServiceRolePolicy	1770
이 정책 사용	1770
정책 세부 정보	1770
정책 버전	1770
JSON 정책 문서	1770
자세히 알아보기	1772
AWSDeviceFarmTestGridServiceRolePolicy	1772
이 정책 사용	1773
정책 세부 정보	1773
정책 버전	1773
JSON 정책 문서	1773
자세히 알아보기	1775

AWSDirectConnectFullAccess	1775
이 정책 사용	1775
정책 세부 정보	1776
정책 버전	1776
JSON 정책 문서	1776
자세히 알아보기	1776
AWSDirectConnectReadOnlyAccess	1777
이 정책 사용	1777
정책 세부 정보	1777
정책 버전	1777
JSON 정책 문서	1777
자세히 알아보기	1778
AWSDirectConnectServiceRolePolicy	1778
이 정책 사용	1778
정책 세부 정보	1778
정책 버전	1778
JSON 정책 문서	1779
자세히 알아보기	1779
AWSDirectoryServiceFullAccess	1779
이 정책 사용	1779
정책 세부 정보	1780
정책 버전	1780
JSON 정책 문서	1780
자세히 알아보기	1782
AWSDirectoryServiceReadOnlyAccess	1782
이 정책 사용	1782
정책 세부 정보	1782
정책 버전	1782
JSON 정책 문서	1783
자세히 알아보기	1783
AWSDiscoveryContinuousExportFirehosePolicy	1784
이 정책 사용	1784
정책 세부 정보	1784
정책 버전	1784
JSON 정책 문서	1784
자세히 알아보기	1785

AWSDMSFleetAdvisorServiceRolePolicy	1785
이 정책 사용	1786
정책 세부 정보	1786
정책 버전	1786
JSON 정책 문서	1786
자세히 알아보기	1787
AWSDMSServerlessServiceRolePolicy	1787
이 정책 사용	1787
정책 세부 정보	1787
정책 버전	1787
JSON 정책 문서	1787
자세히 알아보기	1789
AWSEC2CapacityReservationFleetRolePolicy	1789
이 정책 사용	1789
정책 세부 정보	1789
정책 버전	1790
JSON 정책 문서	1790
자세히 알아보기	1791
AWSEC2FleetServiceRolePolicy	1791
이 정책 사용	1791
정책 세부 정보	1791
정책 버전	1792
JSON 정책 문서	1792
자세히 알아보기	1794
AWSEC2SpotFleetServiceRolePolicy	1794
이 정책 사용	1794
정책 세부 정보	1794
정책 버전	1794
JSON 정책 문서	1795
자세히 알아보기	1797
AWSEC2SpotServiceRolePolicy	1797
이 정책 사용	1797
정책 세부 정보	1797
정책 버전	1797
JSON 정책 문서	1797
자세히 알아보기	1799

AWSEC2VssSnapshotPolicy	1799
이 정책 사용	1799
정책 세부 정보	1799
정책 버전	1800
JSON 정책 문서	1800
자세히 알아보기	1803
AWSECRPullThroughCache_ServiceRolePolicy	1803
이 정책 사용	1803
정책 세부 정보	1803
정책 버전	1804
JSON 정책 문서	1804
자세히 알아보기	1805
AWSElasticBeanstalkCustomPlatformforEC2Role	1805
이 정책 사용	1805
정책 세부 정보	1805
정책 버전	1805
JSON 정책 문서	1806
자세히 알아보기	1807
AWSElasticBeanstalkEnhancedHealth	1807
이 정책 사용	1808
정책 세부 정보	1808
정책 버전	1808
JSON 정책 문서	1808
자세히 알아보기	1809
AWSElasticBeanstalkMaintenance	1809
이 정책 사용	1809
정책 세부 정보	1810
정책 버전	1810
JSON 정책 문서	1810
자세히 알아보기	1811
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	1811
이 정책 사용	1811
정책 세부 정보	1811
정책 버전	1812
JSON 정책 문서	1812
자세히 알아보기	1818

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	1819
이 정책 사용	1819
정책 세부 정보	1819
정책 버전	1819
JSON 정책 문서	1819
자세히 알아보기	1825
AWSElasticBeanstalkMulticontainerDocker	1825
이 정책 사용	1825
정책 세부 정보	1825
정책 버전	1825
JSON 정책 문서	1825
자세히 알아보기	1826
AWSElasticBeanstalkReadOnly	1827
이 정책 사용	1827
정책 세부 정보	1827
정책 버전	1827
JSON 정책 문서	1827
자세히 알아보기	1829
AWSElasticBeanstalkRoleCore	1830
이 정책 사용	1830
정책 세부 정보	1830
정책 버전	1830
JSON 정책 문서	1830
자세히 알아보기	1835
AWSElasticBeanstalkRoleCWL	1835
이 정책 사용	1835
정책 세부 정보	1836
정책 버전	1836
JSON 정책 문서	1836
자세히 알아보기	1836
AWSElasticBeanstalkRoleECS	1837
이 정책 사용	1837
정책 세부 정보	1837
정책 버전	1837
JSON 정책 문서	1837
자세히 알아보기	1838

AWSElasticBeanstalkRoleRDS	1838
이 정책 사용	1839
정책 세부 정보	1839
정책 버전	1839
JSON 정책 문서	1839
자세히 알아보기	1840
AWSElasticBeanstalkRoleSNS	1840
이 정책 사용	1840
정책 세부 정보	1840
정책 버전	1840
JSON 정책 문서	1841
자세히 알아보기	1841
AWSElasticBeanstalkRoleWorkerTier	1842
이 정책 사용	1842
정책 세부 정보	1842
정책 버전	1842
JSON 정책 문서	1842
자세히 알아보기	1843
AWSElasticBeanstalkService	1843
이 정책 사용	1843
정책 세부 정보	1843
정책 버전	1844
JSON 정책 문서	1844
자세히 알아보기	1848
AWSElasticBeanstalkServiceRolePolicy	1848
이 정책 사용	1849
정책 세부 정보	1849
정책 버전	1849
JSON 정책 문서	1849
자세히 알아보기	1851
AWSElasticBeanstalkWebTier	1851
이 정책 사용	1851
정책 세부 정보	1851
정책 버전	1851
JSON 정책 문서	1851
자세히 알아보기	1853

AWSElasticBeanstalkWorkerTier	1853
이 정책 사용	1853
정책 세부 정보	1853
정책 버전	1853
JSON 정책 문서	1854
자세히 알아보기	1856
AWSElasticDisasterRecoveryAgentInstallationPolicy	1856
이 정책 사용	1856
정책 세부 정보	1856
정책 버전	1857
JSON 정책 문서	1857
자세히 알아보기	1858
AWSElasticDisasterRecoveryAgentPolicy	1858
이 정책 사용	1859
정책 세부 정보	1859
정책 버전	1859
JSON 정책 문서	1859
자세히 알아보기	1860
AWSElasticDisasterRecoveryConsoleFullAccess	1860
이 정책 사용	1860
정책 세부 정보	1860
정책 버전	1861
JSON 정책 문서	1861
자세히 알아보기	1870
AWSElasticDisasterRecoveryConsoleFullAccess_v2	1871
이 정책 사용	1871
정책 세부 정보	1871
정책 버전	1871
JSON 정책 문서	1871
자세히 알아보기	1884
AWSElasticDisasterRecoveryConversionServerPolicy	1884
이 정책 사용	1885
정책 세부 정보	1885
정책 버전	1885
JSON 정책 문서	1885
자세히 알아보기	1886

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	1886
이 정책 사용	1886
정책 세부 정보	1886
정책 버전	1886
JSON 정책 문서	1887
자세히 알아보기	1887
AWSElasticDisasterRecoveryEc2InstancePolicy	1888
이 정책 사용	1888
정책 세부 정보	1888
정책 버전	1888
JSON 정책 문서	1888
자세히 알아보기	1890
AWSElasticDisasterRecoveryFailbackInstallationPolicy	1891
이 정책 사용	1891
정책 세부 정보	1891
정책 버전	1891
JSON 정책 문서	1891
자세히 알아보기	1892
AWSElasticDisasterRecoveryFailbackPolicy	1892
이 정책 사용	1893
정책 세부 정보	1893
정책 버전	1893
JSON 정책 문서	1893
자세히 알아보기	1894
AWSElasticDisasterRecoveryLaunchActionsPolicy	1895
이 정책 사용	1895
정책 세부 정보	1895
정책 버전	1895
JSON 정책 문서	1895
자세히 알아보기	1901
AWSElasticDisasterRecoveryNetworkReplicationPolicy	1901
이 정책 사용	1902
정책 세부 정보	1902
정책 버전	1902
JSON 정책 문서	1902
자세히 알아보기	1903

AWSElasticDisasterRecoveryReadOnlyAccess	1903
이 정책 사용	1903
정책 세부 정보	1903
정책 버전	1904
JSON 정책 문서	1904
자세히 알아보기	1906
AWSElasticDisasterRecoveryRecoveryInstancePolicy	1906
이 정책 사용	1906
정책 세부 정보	1906
정책 버전	1907
JSON 정책 문서	1907
자세히 알아보기	1909
AWSElasticDisasterRecoveryReplicationServerPolicy	1910
이 정책 사용	1910
정책 세부 정보	1910
정책 버전	1910
JSON 정책 문서	1910
자세히 알아보기	1913
AWSElasticDisasterRecoveryServiceRolePolicy	1913
이 정책 사용	1913
정책 세부 정보	1913
정책 버전	1913
JSON 정책 문서	1914
자세히 알아보기	1922
AWSElasticDisasterRecoveryStagingAccountPolicy	1922
이 정책 사용	1922
정책 세부 정보	1922
정책 버전	1923
JSON 정책 문서	1923
자세히 알아보기	1924
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	1924
이 정책 사용	1924
정책 세부 정보	1924
정책 버전	1925
JSON 정책 문서	1925
자세히 알아보기	1926

AWSElasticLoadBalancingClassicServiceRolePolicy	1926
이 정책 사용	1926
정책 세부 정보	1926
정책 버전	1927
JSON 정책 문서	1927
자세히 알아보기	1928
AWSElasticLoadBalancingServiceRolePolicy	1928
이 정책 사용	1928
정책 세부 정보	1928
정책 버전	1928
JSON 정책 문서	1928
자세히 알아보기	1930
AWSElementalMediaConvertFullAccess	1930
이 정책 사용	1930
정책 세부 정보	1930
정책 버전	1930
JSON 정책 문서	1930
자세히 알아보기	1931
AWSElementalMediaConvertReadOnly	1931
이 정책 사용	1932
정책 세부 정보	1932
정책 버전	1932
JSON 정책 문서	1932
자세히 알아보기	1933
AWSElementalMediaLiveFullAccess	1933
이 정책 사용	1933
정책 세부 정보	1933
정책 버전	1933
JSON 정책 문서	1933
자세히 알아보기	1934
AWSElementalMediaLiveReadOnly	1934
이 정책 사용	1934
정책 세부 정보	1934
정책 버전	1934
JSON 정책 문서	1935
자세히 알아보기	1935

AWSElementalMediaPackageFullAccess	1935
이 정책 사용	1935
정책 세부 정보	1935
정책 버전	1936
JSON 정책 문서	1936
자세히 알아보기	1936
AWSElementalMediaPackageReadOnly	1936
이 정책 사용	1936
정책 세부 정보	1936
정책 버전	1937
JSON 정책 문서	1937
자세히 알아보기	1937
AWSElementalMediaPackageV2FullAccess	1937
이 정책 사용	1938
정책 세부 정보	1938
정책 버전	1938
JSON 정책 문서	1938
자세히 알아보기	1938
AWSElementalMediaPackageV2ReadOnly	1939
이 정책 사용	1939
정책 세부 정보	1939
정책 버전	1939
JSON 정책 문서	1939
자세히 알아보기	1940
AWSElementalMediaStoreFullAccess	1940
이 정책 사용	1940
정책 세부 정보	1940
정책 버전	1940
JSON 정책 문서	1940
자세히 알아보기	1941
AWSElementalMediaStoreReadOnly	1941
이 정책 사용	1941
정책 세부 정보	1941
정책 버전	1942
JSON 정책 문서	1942
자세히 알아보기	1942

AWSElementalMediaTailorFullAccess	1942
이 정책 사용	1943
정책 세부 정보	1943
정책 버전	1943
JSON 정책 문서	1943
자세히 알아보기	1943
AWSElementalMediaTailorReadOnly	1944
이 정책 사용	1944
정책 세부 정보	1944
정책 버전	1944
JSON 정책 문서	1944
자세히 알아보기	1945
AWSEnhancedClassicNetworkingMangementPolicy	1945
이 정책 사용	1945
정책 세부 정보	1945
정책 버전	1945
JSON 정책 문서	1945
자세히 알아보기	1946
AWSEntityResolutionConsoleFullAccess	1946
이 정책 사용	1946
정책 세부 정보	1946
정책 버전	1946
JSON 정책 문서	1947
자세히 알아보기	1949
AWSEntityResolutionConsoleReadOnlyAccess	1950
이 정책 사용	1950
정책 세부 정보	1950
정책 버전	1950
JSON 정책 문서	1950
자세히 알아보기	1951
AWSFaultInjectionSimulatorEC2Access	1951
이 정책 사용	1951
정책 세부 정보	1951
정책 버전	1951
JSON 정책 문서	1952
자세히 알아보기	1953

AWSFaultInjectionSimulatorECSAccess	1953
이 정책 사용	1953
정책 세부 정보	1954
정책 버전	1954
JSON 정책 문서	1954
자세히 알아보기	1956
AWSFaultInjectionSimulatorEKSAccess	1956
이 정책 사용	1956
정책 세부 정보	1956
정책 버전	1956
JSON 정책 문서	1957
자세히 알아보기	1958
AWSFaultInjectionSimulatorNetworkAccess	1958
이 정책 사용	1958
정책 세부 정보	1958
정책 버전	1958
JSON 정책 문서	1959
자세히 알아보기	1966
AWSFaultInjectionSimulatorRDSAccess	1966
이 정책 사용	1966
정책 세부 정보	1966
정책 버전	1966
JSON 정책 문서	1966
자세히 알아보기	1968
AWSFaultInjectionSimulatorSSMAccess	1968
이 정책 사용	1968
정책 세부 정보	1968
정책 버전	1968
JSON 정책 문서	1968
자세히 알아보기	1970
AWSFinSpaceServiceRolePolicy	1970
이 정책 사용	1970
정책 세부 정보	1970
정책 버전	1970
JSON 정책 문서	1971
자세히 알아보기	1971

AWSFMAdminFullAccess	1971
이 정책 사용	1971
정책 세부 정보	1972
정책 버전	1972
JSON 정책 문서	1972
자세히 알아보기	1974
AWSFMAdminReadOnlyAccess	1974
이 정책 사용	1974
정책 세부 정보	1974
정책 버전	1974
JSON 정책 문서	1975
자세히 알아보기	1976
AWSFMMemberReadOnlyAccess	1976
이 정책 사용	1976
정책 세부 정보	1977
정책 버전	1977
JSON 정책 문서	1977
자세히 알아보기	1977
AWSForWordPressPluginPolicy	1978
이 정책 사용	1978
정책 세부 정보	1978
정책 버전	1978
JSON 정책 문서	1978
자세히 알아보기	1980
AWSGitSyncServiceRolePolicy	1980
이 정책 사용	1980
정책 세부 정보	1981
정책 버전	1981
JSON 정책 문서	1981
자세히 알아보기	1982
AWSGlobalAcceleratorSLRPolicy	1982
이 정책 사용	1982
정책 세부 정보	1982
정책 버전	1982
JSON 정책 문서	1982
자세히 알아보기	1984

AWSGlueConsoleFullAccess	1984
이 정책 사용	1984
정책 세부 정보	1984
정책 버전	1985
JSON 정책 문서	1985
자세히 알아보기	1989
AWSGlueConsoleSageMakerNotebookFullAccess	1989
이 정책 사용	1989
정책 세부 정보	1989
정책 버전	1990
JSON 정책 문서	1990
자세히 알아보기	1995
AwsGlueDataBrewFullAccessPolicy	1995
이 정책 사용	1995
정책 세부 정보	1995
정책 버전	1996
JSON 정책 문서	1996
자세히 알아보기	2001
AWSGlueDataBrewServiceRole	2001
이 정책 사용	2001
정책 세부 정보	2001
정책 버전	2002
JSON 정책 문서	2002
자세히 알아보기	2005
AWSGlueSchemaRegistryFullAccess	2005
이 정책 사용	2005
정책 세부 정보	2005
정책 버전	2005
JSON 정책 문서	2005
자세히 알아보기	2007
AWSGlueSchemaRegistryReadOnlyAccess	2007
이 정책 사용	2007
정책 세부 정보	2007
정책 버전	2007
JSON 정책 문서	2007
자세히 알아보기	2008

AWSGlueServiceNotebookRole	2008
이 정책 사용	2008
정책 세부 정보	2009
정책 버전	2009
JSON 정책 문서	2009
자세히 알아보기	2011
AWSGlueServiceRole	2012
이 정책 사용	2012
정책 세부 정보	2012
정책 버전	2012
JSON 정책 문서	2012
자세히 알아보기	2014
AwsGlueSessionUserRestrictedNotebookPolicy	2015
이 정책 사용	2015
정책 세부 정보	2015
정책 버전	2015
JSON 정책 문서	2015
자세히 알아보기	2018
AwsGlueSessionUserRestrictedNotebookServiceRole	2018
이 정책 사용	2018
정책 세부 정보	2018
정책 버전	2019
JSON 정책 문서	2019
자세히 알아보기	2022
AwsGlueSessionUserRestrictedPolicy	2023
이 정책 사용	2023
정책 세부 정보	2023
정책 버전	2023
JSON 정책 문서	2023
자세히 알아보기	2026
AwsGlueSessionUserRestrictedServiceRole	2026
이 정책 사용	2026
정책 세부 정보	2026
정책 버전	2026
JSON 정책 문서	2027
자세히 알아보기	2031

AWSGrafanaAccountAdministrator	2031
이 정책 사용	2031
정책 세부 정보	2031
정책 버전	2031
JSON 정책 문서	2032
자세히 알아보기	2033
AWSGrafanaConsoleReadOnlyAccess	2033
이 정책 사용	2033
정책 세부 정보	2033
정책 버전	2033
JSON 정책 문서	2033
자세히 알아보기	2034
AWSGrafanaWorkspacePermissionManagement	2034
이 정책 사용	2034
정책 세부 정보	2034
정책 버전	2035
JSON 정책 문서	2035
자세히 알아보기	2036
AWSGrafanaWorkspacePermissionManagementV2	2036
이 정책 사용	2036
정책 세부 정보	2036
정책 버전	2036
JSON 정책 문서	2037
자세히 알아보기	2037
AWSGreengrassFullAccess	2038
이 정책 사용	2038
정책 세부 정보	2038
정책 버전	2038
JSON 정책 문서	2038
자세히 알아보기	2039
AWSGreengrassReadOnlyAccess	2039
이 정책 사용	2039
정책 세부 정보	2039
정책 버전	2039
JSON 정책 문서	2040
자세히 알아보기	2040

AWSGreengrassResourceAccessRolePolicy	2040
이 정책 사용	2040
정책 세부 정보	2040
정책 버전	2041
JSON 정책 문서	2041
자세히 알아보기	2043
AWSGroundStationAgentInstancePolicy	2043
이 정책 사용	2043
정책 세부 정보	2044
정책 버전	2044
JSON 정책 문서	2044
자세히 알아보기	2044
AWSHealth_EventProcessorServiceRolePolicy	2045
이 정책 사용	2045
정책 세부 정보	2045
정책 버전	2045
JSON 정책 문서	2045
자세히 알아보기	2046
AWSHealthFullAccess	2046
이 정책 사용	2046
정책 세부 정보	2046
정책 버전	2047
JSON 정책 문서	2047
자세히 알아보기	2048
AWSHealthImagingFullAccess	2048
이 정책 사용	2048
정책 세부 정보	2048
정책 버전	2048
JSON 정책 문서	2049
자세히 알아보기	2049
AWSHealthImagingReadOnlyAccess	2049
이 정책 사용	2050
정책 세부 정보	2050
정책 버전	2050
JSON 정책 문서	2050
자세히 알아보기	2051

AWSIAMIdentityCenterAllowListForIdentityContext	2051
이 정책 사용	2051
정책 세부 정보	2051
정책 버전	2051
JSON 정책 문서	2052
자세히 알아보기	2054
AWSIdentitySyncFullAccess	2055
이 정책 사용	2055
정책 세부 정보	2055
정책 버전	2055
JSON 정책 문서	2055
자세히 알아보기	2056
AWSIdentitySyncReadOnlyAccess	2056
이 정책 사용	2056
정책 세부 정보	2056
정책 버전	2057
JSON 정책 문서	2057
자세히 알아보기	2057
AWSImageBuilderFullAccess	2058
이 정책 사용	2058
정책 세부 정보	2058
정책 버전	2058
JSON 정책 문서	2058
자세히 알아보기	2061
AWSImageBuilderReadOnlyAccess	2061
이 정책 사용	2061
정책 세부 정보	2061
정책 버전	2062
JSON 정책 문서	2062
자세히 알아보기	2062
AWSImportExportFullAccess	2063
이 정책 사용	2063
정책 세부 정보	2063
정책 버전	2063
JSON 정책 문서	2063
자세히 알아보기	2064

AWSImportExportReadOnlyAccess	2064
이 정책 사용	2064
정책 세부 정보	2064
정책 버전	2064
JSON 정책 문서	2064
자세히 알아보기	2065
AWSIncidentManagerIncidentAccessServiceRolePolicy	2065
이 정책 사용	2065
정책 세부 정보	2065
정책 버전	2066
JSON 정책 문서	2066
자세히 알아보기	2066
AWSIncidentManagerResolverAccess	2067
이 정책 사용	2067
정책 세부 정보	2067
정책 버전	2067
JSON 정책 문서	2067
자세히 알아보기	2068
AWSIncidentManagerServiceRolePolicy	2068
이 정책 사용	2069
정책 세부 정보	2069
정책 버전	2069
JSON 정책 문서	2069
자세히 알아보기	2070
AWSIoT1ClickFullAccess	2070
이 정책 사용	2071
정책 세부 정보	2071
정책 버전	2071
JSON 정책 문서	2071
자세히 알아보기	2071
AWSIoT1ClickReadOnlyAccess	2072
이 정책 사용	2072
정책 세부 정보	2072
정책 버전	2072
JSON 정책 문서	2072
자세히 알아보기	2073

AWSIoTAnalyticsFullAccess	2073
이 정책 사용	2073
정책 세부 정보	2073
정책 버전	2073
JSON 정책 문서	2074
자세히 알아보기	2074
AWSIoTAnalyticsReadOnlyAccess	2074
이 정책 사용	2074
정책 세부 정보	2074
정책 버전	2075
JSON 정책 문서	2075
자세히 알아보기	2075
AWSIoTConfigAccess	2075
이 정책 사용	2076
정책 세부 정보	2076
정책 버전	2076
JSON 정책 문서	2076
자세히 알아보기	2080
AWSIoTConfigReadOnlyAccess	2080
이 정책 사용	2080
정책 세부 정보	2080
정책 버전	2081
JSON 정책 문서	2081
자세히 알아보기	2083
AWSIoTDataAccess	2083
이 정책 사용	2083
정책 세부 정보	2083
정책 버전	2083
JSON 정책 문서	2084
자세히 알아보기	2084
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	2084
이 정책 사용	2085
정책 세부 정보	2085
정책 버전	2085
JSON 정책 문서	2085
자세히 알아보기	2086

AWSIoTDeviceDefenderAudit	2086
이 정책 사용	2086
정책 세부 정보	2086
정책 버전	2086
JSON 정책 문서	2086
자세히 알아보기	2087
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	2088
이 정책 사용	2088
정책 세부 정보	2088
정책 버전	2088
JSON 정책 문서	2088
자세히 알아보기	2089
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	2089
이 정책 사용	2089
정책 세부 정보	2090
정책 버전	2090
JSON 정책 문서	2090
자세히 알아보기	2090
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	2091
이 정책 사용	2091
정책 세부 정보	2091
정책 버전	2091
JSON 정책 문서	2091
자세히 알아보기	2092
AWSIoTDeviceDefenderUpdateCACertMitigationAction	2092
이 정책 사용	2092
정책 세부 정보	2092
정책 버전	2093
JSON 정책 문서	2093
자세히 알아보기	2093
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	2093
이 정책 사용	2094
정책 세부 정보	2094
정책 버전	2094
JSON 정책 문서	2094
자세히 알아보기	2095

AWSIoTDeviceTesterForFreeRTOSFullAccess	2095
이 정책 사용	2095
정책 세부 정보	2095
정책 버전	2095
JSON 정책 문서	2095
자세히 알아보기	2102
AWSIoTDeviceTesterForGreengrassFullAccess	2102
이 정책 사용	2102
정책 세부 정보	2102
정책 버전	2102
JSON 정책 문서	2102
자세히 알아보기	2105
AWSIoTEventsFullAccess	2106
이 정책 사용	2106
정책 세부 정보	2106
정책 버전	2106
JSON 정책 문서	2106
자세히 알아보기	2107
AWSIoTEventsReadOnlyAccess	2107
이 정책 사용	2107
정책 세부 정보	2107
정책 버전	2107
JSON 정책 문서	2107
자세히 알아보기	2108
AWSIoTFleetHubFederationAccess	2108
이 정책 사용	2108
정책 세부 정보	2108
정책 버전	2108
JSON 정책 문서	2109
자세히 알아보기	2110
AWSIoTFleetwiseServiceRolePolicy	2111
이 정책 사용	2111
정책 세부 정보	2111
정책 버전	2111
JSON 정책 문서	2111
자세히 알아보기	2112

AWSIoTFullAccess	2112
이 정책 사용	2112
정책 세부 정보	2112
정책 버전	2112
JSON 정책 문서	2113
자세히 알아보기	2113
AWSIoTLogging	2113
이 정책 사용	2113
정책 세부 정보	2113
정책 버전	2114
JSON 정책 문서	2114
자세히 알아보기	2114
AWSIoTOTAUpdate	2115
이 정책 사용	2115
정책 세부 정보	2115
정책 버전	2115
JSON 정책 문서	2115
자세히 알아보기	2116
AWSIoTRoboRunnerFullAccess	2116
이 정책 사용	2116
정책 세부 정보	2116
정책 버전	2116
JSON 정책 문서	2116
자세히 알아보기	2117
AWSIoTRoboRunnerReadOnly	2117
이 정책 사용	2117
정책 세부 정보	2117
정책 버전	2118
JSON 정책 문서	2118
자세히 알아보기	2118
AWSIoTRoboRunnerServiceRolePolicy	2119
이 정책 사용	2119
정책 세부 정보	2119
정책 버전	2119
JSON 정책 문서	2119
자세히 알아보기	2120

AWSIoTRuleActions	2120
이 정책 사용	2120
정책 세부 정보	2120
정책 버전	2120
JSON 정책 문서	2121
자세히 알아보기	2121
AWSIoTSiteWiseConsoleFullAccess	2121
이 정책 사용	2122
정책 세부 정보	2122
정책 버전	2122
JSON 정책 문서	2122
자세히 알아보기	2124
AWSIoTSiteWiseFullAccess	2124
이 정책 사용	2124
정책 세부 정보	2125
정책 버전	2125
JSON 정책 문서	2125
자세히 알아보기	2125
AWSIoTSiteWiseMonitorPortalAccess	2126
이 정책 사용	2126
정책 세부 정보	2126
정책 버전	2126
JSON 정책 문서	2126
자세히 알아보기	2127
AWSIoTSiteWiseMonitorServiceRolePolicy	2127
이 정책 사용	2128
정책 세부 정보	2128
정책 버전	2128
JSON 정책 문서	2128
자세히 알아보기	2129
AWSIoTSiteWiseReadOnlyAccess	2129
이 정책 사용	2129
정책 세부 정보	2129
정책 버전	2130
JSON 정책 문서	2130
자세히 알아보기	2130

AWSIoTThingsRegistration	2131
이 정책 사용	2131
정책 세부 정보	2131
정책 버전	2131
JSON 정책 문서	2131
자세히 알아보기	2132
AWSIoTTwinMakerServiceRolePolicy	2133
이 정책 사용	2133
정책 세부 정보	2133
정책 버전	2133
JSON 정책 문서	2133
자세히 알아보기	2135
AWSIoTWirelessDataAccess	2135
이 정책 사용	2135
정책 세부 정보	2135
정책 버전	2135
JSON 정책 문서	2136
자세히 알아보기	2136
AWSIoTWirelessFullAccess	2136
이 정책 사용	2136
정책 세부 정보	2136
정책 버전	2137
JSON 정책 문서	2137
자세히 알아보기	2137
AWSIoTWirelessFullPublishAccess	2137
이 정책 사용	2138
정책 세부 정보	2138
정책 버전	2138
JSON 정책 문서	2138
자세히 알아보기	2138
AWSIoTWirelessGatewayCertManager	2139
이 정책 사용	2139
정책 세부 정보	2139
정책 버전	2139
JSON 정책 문서	2139
자세히 알아보기	2140

AWSIoTWirelessLogging	2140
이 정책 사용	2140
정책 세부 정보	2140
정책 버전	2140
JSON 정책 문서	2141
자세히 알아보기	2141
AWSIoTWirelessReadOnlyAccess	2141
이 정책 사용	2141
정책 세부 정보	2142
정책 버전	2142
JSON 정책 문서	2142
자세히 알아보기	2142
AWSIPAMServiceRolePolicy	2143
이 정책 사용	2143
정책 세부 정보	2143
정책 버전	2143
JSON 정책 문서	2143
자세히 알아보기	2144
AWSIQContractServiceRolePolicy	2144
이 정책 사용	2145
정책 세부 정보	2145
정책 버전	2145
JSON 정책 문서	2145
자세히 알아보기	2146
AWSIQFullAccess	2146
이 정책 사용	2146
정책 세부 정보	2146
정책 버전	2146
JSON 정책 문서	2146
자세히 알아보기	2147
AWSIQPermissionServiceRolePolicy	2147
이 정책 사용	2147
정책 세부 정보	2148
정책 버전	2148
JSON 정책 문서	2148
자세히 알아보기	2149

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2149
이 정책 사용	2149
정책 세부 정보	2149
정책 버전	2149
JSON 정책 문서	2150
자세히 알아보기	2150
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2150
이 정책 사용	2151
정책 세부 정보	2151
정책 버전	2151
JSON 정책 문서	2151
자세히 알아보기	2151
AWSKeyManagementServicePowerUser	2152
이 정책 사용	2152
정책 세부 정보	2152
정책 버전	2152
JSON 정책 문서	2152
자세히 알아보기	2153
AWSLakeFormationCrossAccountManager	2153
이 정책 사용	2153
정책 세부 정보	2153
정책 버전	2154
JSON 정책 문서	2154
자세히 알아보기	2156
AWSLakeFormationDataAdmin	2156
이 정책 사용	2156
정책 세부 정보	2156
정책 버전	2156
JSON 정책 문서	2157
자세히 알아보기	2158
AWSLambda_FullAccess	2158
이 정책 사용	2158
정책 세부 정보	2158
정책 버전	2159
JSON 정책 문서	2159
자세히 알아보기	2160

AWSLambda_ReadOnlyAccess	2160
이 정책 사용	2160
정책 세부 정보	2161
정책 버전	2161
JSON 정책 문서	2161
자세히 알아보기	2162
AWSLambdaBasicExecutionRole	2162
이 정책 사용	2163
정책 세부 정보	2163
정책 버전	2163
JSON 정책 문서	2163
자세히 알아보기	2163
AWSLambdaDynamoDBExecutionRole	2164
이 정책 사용	2164
정책 세부 정보	2164
정책 버전	2164
JSON 정책 문서	2164
자세히 알아보기	2165
AWSLambdaENIManagementAccess	2165
이 정책 사용	2165
정책 세부 정보	2165
정책 버전	2166
JSON 정책 문서	2166
자세히 알아보기	2166
AWSLambdaExecute	2166
이 정책 사용	2167
정책 세부 정보	2167
정책 버전	2167
JSON 정책 문서	2167
자세히 알아보기	2168
AWSLambdaFullAccess	2168
이 정책 사용	2168
정책 세부 정보	2168
정책 버전	2168
JSON 정책 문서	2169
자세히 알아보기	2170

AWSLambdaInvocation-DynamoDB	2170
이 정책 사용	2170
정책 세부 정보	2171
정책 버전	2171
JSON 정책 문서	2171
자세히 알아보기	2172
AWSLambdaKinesisExecutionRole	2172
이 정책 사용	2172
정책 세부 정보	2172
정책 버전	2172
JSON 정책 문서	2172
자세히 알아보기	2173
AWSLambdaMSKExecutionRole	2173
이 정책 사용	2173
정책 세부 정보	2174
정책 버전	2174
JSON 정책 문서	2174
자세히 알아보기	2175
AWSLambdaReplicator	2175
이 정책 사용	2175
정책 세부 정보	2175
정책 버전	2175
JSON 정책 문서	2175
자세히 알아보기	2177
AWSLambdaRole	2177
이 정책 사용	2177
정책 세부 정보	2177
정책 버전	2177
JSON 정책 문서	2177
자세히 알아보기	2178
AWSLambdaSQSQueueExecutionRole	2178
이 정책 사용	2178
정책 세부 정보	2178
정책 버전	2178
JSON 정책 문서	2179
자세히 알아보기	2179

AWSLambdaVPCAccessExecutionRole	2179
이 정책 사용	2180
정책 세부 정보	2180
정책 버전	2180
JSON 정책 문서	2180
자세히 알아보기	2181
AWSLicenseManagerConsumptionPolicy	2181
이 정책 사용	2181
정책 세부 정보	2181
정책 버전	2181
JSON 정책 문서	2182
자세히 알아보기	2182
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	2182
이 정책 사용	2182
정책 세부 정보	2182
정책 버전	2183
JSON 정책 문서	2183
자세히 알아보기	2184
AWSLicenseManagerMasterAccountRolePolicy	2184
이 정책 사용	2184
정책 세부 정보	2184
정책 버전	2184
JSON 정책 문서	2185
자세히 알아보기	2189
AWSLicenseManagerMemberAccountRolePolicy	2190
이 정책 사용	2190
정책 세부 정보	2190
정책 버전	2190
JSON 정책 문서	2190
자세히 알아보기	2191
AWSLicenseManagerServiceRolePolicy	2191
이 정책 사용	2192
정책 세부 정보	2192
정책 버전	2192
JSON 정책 문서	2192
자세히 알아보기	2195

AWSLicenseManagerUserSubscriptionsServiceRolePolicy	2196
이 정책 사용	2196
정책 세부 정보	2196
정책 버전	2196
JSON 정책 문서	2196
자세히 알아보기	2198
AWSM2ServicePolicy	2198
이 정책 사용	2198
정책 세부 정보	2199
정책 버전	2199
JSON 정책 문서	2199
자세히 알아보기	2200
AWSManagedServices_ContactsServiceRolePolicy	2200
이 정책 사용	2201
정책 세부 정보	2201
정책 버전	2201
JSON 정책 문서	2201
자세히 알아보기	2202
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	2202
이 정책 사용	2202
정책 세부 정보	2202
정책 버전	2203
JSON 정책 문서	2203
자세히 알아보기	2204
AWSManagedServices_EventsServiceRolePolicy	2204
이 정책 사용	2205
정책 세부 정보	2205
정책 버전	2205
JSON 정책 문서	2205
자세히 알아보기	2206
AWSManagedServicesDeploymentToolkitPolicy	2206
이 정책 사용	2206
정책 세부 정보	2206
정책 버전	2207
JSON 정책 문서	2207
자세히 알아보기	2209

AWSMarketplaceAmilngestion	2209
이 정책 사용	2209
정책 세부 정보	2209
정책 버전	2209
JSON 정책 문서	2210
자세히 알아보기	2210
AWSMarketplaceDeploymentServiceRolePolicy	2211
이 정책 사용	2211
정책 세부 정보	2211
정책 버전	2211
JSON 정책 문서	2211
자세히 알아보기	2213
AWSMarketplaceFullAccess	2213
이 정책 사용	2213
정책 세부 정보	2213
정책 버전	2213
JSON 정책 문서	2213
자세히 알아보기	2217
AWSMarketplaceGetEntitlements	2217
이 정책 사용	2217
정책 세부 정보	2217
정책 버전	2217
JSON 정책 문서	2217
자세히 알아보기	2218
AWSMarketplaceImageBuildFullAccess	2218
이 정책 사용	2218
정책 세부 정보	2218
정책 버전	2219
JSON 정책 문서	2219
자세히 알아보기	2222
AWSMarketplaceLicenseManagementServiceRolePolicy	2222
이 정책 사용	2223
정책 세부 정보	2223
정책 버전	2223
JSON 정책 문서	2223
자세히 알아보기	2224

AWSMarketplaceManageSubscriptions	2224
이 정책 사용	2224
정책 세부 정보	2224
정책 버전	2224
JSON 정책 문서	2225
자세히 알아보기	2225
AWSMarketplaceMeteringFullAccess	2226
이 정책 사용	2226
정책 세부 정보	2226
정책 버전	2226
JSON 정책 문서	2226
자세히 알아보기	2227
AWSMarketplaceMeteringRegisterUsage	2227
이 정책 사용	2227
정책 세부 정보	2227
정책 버전	2227
JSON 정책 문서	2227
자세히 알아보기	2228
AWSMarketplaceProcurementSystemAdminFullAccess	2228
이 정책 사용	2228
정책 세부 정보	2228
정책 버전	2229
JSON 정책 문서	2229
자세히 알아보기	2229
AWSMarketplacePurchaseOrdersServiceRolePolicy	2229
이 정책 사용	2230
정책 세부 정보	2230
정책 버전	2230
JSON 정책 문서	2230
자세히 알아보기	2231
AWSMarketplaceRead-only	2231
이 정책 사용	2231
정책 세부 정보	2231
정책 버전	2231
JSON 정책 문서	2231
자세히 알아보기	2233

AWSMarketplaceResaleAuthorizationServiceRolePolicy	2233
이 정책 사용	2233
정책 세부 정보	2233
정책 버전	2233
JSON 정책 문서	2234
자세히 알아보기	2236
AWSMarketplaceSellerFullAccess	2236
이 정책 사용	2236
정책 세부 정보	2236
정책 버전	2236
JSON 정책 문서	2237
자세히 알아보기	2240
AWSMarketplaceSellerProductsFullAccess	2240
이 정책 사용	2240
정책 세부 정보	2241
정책 버전	2241
JSON 정책 문서	2241
자세히 알아보기	2243
AWSMarketplaceSellerProductsReadOnly	2243
이 정책 사용	2243
정책 세부 정보	2243
정책 버전	2243
JSON 정책 문서	2244
자세히 알아보기	2244
AWSMediaConnectServicePolicy	2245
이 정책 사용	2245
정책 세부 정보	2245
정책 버전	2245
JSON 정책 문서	2245
자세히 알아보기	2246
AWSMediaTailorServiceRolePolicy	2247
이 정책 사용	2247
정책 세부 정보	2247
정책 버전	2247
JSON 정책 문서	2247
자세히 알아보기	2248

AWSMigrationHubDiscoveryAccess	2248
이 정책 사용	2248
정책 세부 정보	2248
정책 버전	2248
JSON 정책 문서	2249
자세히 알아보기	2250
AWSMigrationHubDMSAccess	2250
이 정책 사용	2250
정책 세부 정보	2250
정책 버전	2251
JSON 정책 문서	2251
자세히 알아보기	2252
AWSMigrationHubFullAccess	2252
이 정책 사용	2252
정책 세부 정보	2252
정책 버전	2252
JSON 정책 문서	2253
자세히 알아보기	2254
AWSMigrationHubOrchestratorConsoleFullAccess	2254
이 정책 사용	2254
정책 세부 정보	2254
정책 버전	2255
JSON 정책 문서	2255
자세히 알아보기	2258
AWSMigrationHubOrchestratorInstanceRolePolicy	2258
이 정책 사용	2258
정책 세부 정보	2258
정책 버전	2259
JSON 정책 문서	2259
자세히 알아보기	2259
AWSMigrationHubOrchestratorPlugin	2260
이 정책 사용	2260
정책 세부 정보	2260
정책 버전	2260
JSON 정책 문서	2260
자세히 알아보기	2262

AWSMigrationHubOrchestratorServiceRolePolicy	2262
이 정책 사용	2262
정책 세부 정보	2262
정책 버전	2262
JSON 정책 문서	2263
자세히 알아보기	2266
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	2266
이 정책 사용	2266
정책 세부 정보	2267
정책 버전	2267
JSON 정책 문서	2267
자세히 알아보기	2272
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	2273
이 정책 사용	2273
정책 세부 정보	2273
정책 버전	2273
JSON 정책 문서	2274
자세히 알아보기	2275
AWSMigrationHubRefactorSpacesFullAccess	2275
이 정책 사용	2275
정책 세부 정보	2275
정책 버전	2276
JSON 정책 문서	2276
자세히 알아보기	2282
AWSMigrationHubRefactorSpacesServiceRolePolicy	2282
이 정책 사용	2283
정책 세부 정보	2283
정책 버전	2283
JSON 정책 문서	2283
자세히 알아보기	2287
AWSMigrationHubSMSAccess	2287
이 정책 사용	2287
정책 세부 정보	2287
정책 버전	2287
JSON 정책 문서	2288
자세히 알아보기	2289

AWSMigrationHubStrategyCollector	2289
이 정책 사용	2289
정책 세부 정보	2289
정책 버전	2289
JSON 정책 문서	2290
자세히 알아보기	2292
AWSMigrationHubStrategyConsoleFullAccess	2292
이 정책 사용	2292
정책 세부 정보	2292
정책 버전	2292
JSON 정책 문서	2293
자세히 알아보기	2294
AWSMigrationHubStrategyServiceRolePolicy	2295
이 정책 사용	2295
정책 세부 정보	2295
정책 버전	2295
JSON 정책 문서	2295
자세히 알아보기	2296
AWSMobileHub_FullAccess	2296
이 정책 사용	2297
정책 세부 정보	2297
정책 버전	2297
JSON 정책 문서	2297
자세히 알아보기	2299
AWSMobileHub_ReadOnly	2299
이 정책 사용	2299
정책 세부 정보	2299
정책 버전	2299
JSON 정책 문서	2300
자세히 알아보기	2301
AWSMSKReplicatorExecutionRole	2301
이 정책 사용	2301
정책 세부 정보	2301
정책 버전	2301
JSON 정책 문서	2302
자세히 알아보기	2303

AWSNetworkFirewallServiceRolePolicy	2303
이 정책 사용	2303
정책 세부 정보	2303
정책 버전	2304
JSON 정책 문서	2304
자세히 알아보기	2305
AWSNetworkManagerCloudWANServiceRolePolicy	2306
이 정책 사용	2306
정책 세부 정보	2306
정책 버전	2306
JSON 정책 문서	2306
자세히 알아보기	2307
AWSNetworkManagerFullAccess	2307
이 정책 사용	2307
정책 세부 정보	2307
정책 버전	2307
JSON 정책 문서	2308
자세히 알아보기	2308
AWSNetworkManagerReadOnlyAccess	2308
이 정책 사용	2309
정책 세부 정보	2309
정책 버전	2309
JSON 정책 문서	2309
자세히 알아보기	2309
AWSNetworkManagerServiceRolePolicy	2310
이 정책 사용	2310
정책 세부 정보	2310
정책 버전	2310
JSON 정책 문서	2310
자세히 알아보기	2311
AWSOpsWorks_FullAccess	2312
이 정책 사용	2312
정책 세부 정보	2312
정책 버전	2312
JSON 정책 문서	2312
자세히 알아보기	2313

AWSOpsWorksCloudWatchLogs	2313
이 정책 사용	2314
정책 세부 정보	2314
정책 버전	2314
JSON 정책 문서	2314
자세히 알아보기	2315
AWSOpsWorksCMInstanceProfileRole	2315
이 정책 사용	2315
정책 세부 정보	2315
정책 버전	2315
JSON 정책 문서	2315
자세히 알아보기	2316
AWSOpsWorksCMServiceRole	2317
이 정책 사용	2317
정책 세부 정보	2317
정책 버전	2317
JSON 정책 문서	2317
자세히 알아보기	2321
AWSOpsWorksInstanceRegistration	2322
이 정책 사용	2322
정책 세부 정보	2322
정책 버전	2322
JSON 정책 문서	2322
자세히 알아보기	2323
AWSOpsWorksRegisterCLI_EC2	2323
이 정책 사용	2323
정책 세부 정보	2323
정책 버전	2323
JSON 정책 문서	2324
자세히 알아보기	2324
AWSOpsWorksRegisterCLI_OnPremises	2325
이 정책 사용	2325
정책 세부 정보	2325
정책 버전	2325
JSON 정책 문서	2325
자세히 알아보기	2327

AWSOrganizationsFullAccess	2327
이 정책 사용	2327
정책 세부 정보	2327
정책 버전	2327
JSON 정책 문서	2328
자세히 알아보기	2329
AWSOrganizationsReadOnlyAccess	2329
이 정책 사용	2329
정책 세부 정보	2329
정책 버전	2329
JSON 정책 문서	2329
자세히 알아보기	2330
AWSOrganizationsServiceTrustPolicy	2330
이 정책 사용	2331
정책 세부 정보	2331
정책 버전	2331
JSON 정책 문서	2331
자세히 알아보기	2332
AWSOutpostsAuthorizeServerPolicy	2332
이 정책 사용	2332
정책 세부 정보	2332
정책 버전	2332
JSON 정책 문서	2333
자세히 알아보기	2333
AWSOutpostsServiceRolePolicy	2333
이 정책 사용	2333
정책 세부 정보	2333
정책 버전	2334
JSON 정책 문서	2334
자세히 알아보기	2334
AWSPanoramaApplianceRolePolicy	2334
이 정책 사용	2335
정책 세부 정보	2335
정책 버전	2335
JSON 정책 문서	2335
자세히 알아보기	2336

AWSPanoramaApplianceServiceRolePolicy	2336
이 정책 사용	2336
정책 세부 정보	2336
정책 버전	2336
JSON 정책 문서	2337
자세히 알아보기	2338
AWSPanoramaFullAccess	2338
이 정책 사용	2338
정책 세부 정보	2339
정책 버전	2339
JSON 정책 문서	2339
자세히 알아보기	2341
AWSPanoramaGreengrassGroupRolePolicy	2342
이 정책 사용	2342
정책 세부 정보	2342
정책 버전	2342
JSON 정책 문서	2342
자세히 알아보기	2344
AWSPanoramaSageMakerRolePolicy	2344
이 정책 사용	2344
정책 세부 정보	2344
정책 버전	2344
JSON 정책 문서	2345
자세히 알아보기	2345
AWSPanoramaServiceLinkedRolePolicy	2345
이 정책 사용	2345
정책 세부 정보	2346
정책 버전	2346
JSON 정책 문서	2346
자세히 알아보기	2349
AWSPanoramaServiceRolePolicy	2349
이 정책 사용	2349
정책 세부 정보	2349
정책 버전	2349
JSON 정책 문서	2349
자세히 알아보기	2356

AWSPriceListServiceFullAccess	2357
이 정책 사용	2357
정책 세부 정보	2357
정책 버전	2357
JSON 정책 문서	2357
자세히 알아보기	2358
AWSPrivatCAAuditor	2358
이 정책 사용	2358
정책 세부 정보	2358
정책 버전	2358
JSON 정책 문서	2358
자세히 알아보기	2359
AWSPrivatCAFullAccess	2359
이 정책 사용	2359
정책 세부 정보	2360
정책 버전	2360
JSON 정책 문서	2360
자세히 알아보기	2360
AWSPrivatCAPrivilegedUser	2361
이 정책 사용	2361
정책 세부 정보	2361
정책 버전	2361
JSON 정책 문서	2361
자세히 알아보기	2362
AWSPrivatCAReadOnly	2363
이 정책 사용	2363
정책 세부 정보	2363
정책 버전	2363
JSON 정책 문서	2363
자세히 알아보기	2364
AWSPrivatCAUser	2364
이 정책 사용	2364
정책 세부 정보	2364
정책 버전	2364
JSON 정책 문서	2365
자세히 알아보기	2366

AWSPublicMarketplaceAdminFullAccess	2366
이 정책 사용	2366
정책 세부 정보	2366
정책 버전	2367
JSON 정책 문서	2367
자세히 알아보기	2368
AWSPublicMarketplaceRequests	2368
이 정책 사용	2369
정책 세부 정보	2369
정책 버전	2369
JSON 정책 문서	2369
자세히 알아보기	2369
AWSPublicNetworksServiceRolePolicy	2370
이 정책 사용	2370
정책 세부 정보	2370
정책 버전	2370
JSON 정책 문서	2370
자세히 알아보기	2371
AWSPublicProtonCodeBuildProvisioningBasicAccess	2371
이 정책 사용	2371
정책 세부 정보	2371
정책 버전	2371
JSON 정책 문서	2372
자세히 알아보기	2372
AWSPublicProtonCodeBuildProvisioningServiceRolePolicy	2372
이 정책 사용	2373
정책 세부 정보	2373
정책 버전	2373
JSON 정책 문서	2373
자세히 알아보기	2374
AWSPublicProtonDeveloperAccess	2375
이 정책 사용	2375
정책 세부 정보	2375
정책 버전	2375
JSON 정책 문서	2375
자세히 알아보기	2378

AWSProtonFullAccess	2378
이 정책 사용	2378
정책 세부 정보	2378
정책 버전	2378
JSON 정책 문서	2378
자세히 알아보기	2381
AWSProtonReadOnlyAccess	2381
이 정책 사용	2381
정책 세부 정보	2381
정책 버전	2381
JSON 정책 문서	2381
자세히 알아보기	2383
AWSProtonServiceGitSyncServiceRolePolicy	2383
이 정책 사용	2383
정책 세부 정보	2383
정책 버전	2384
JSON 정책 문서	2384
자세히 알아보기	2384
AWSProtonSyncServiceRolePolicy	2385
이 정책 사용	2385
정책 세부 정보	2385
정책 버전	2385
JSON 정책 문서	2385
자세히 알아보기	2386
AWSPurchaseOrdersServiceRolePolicy	2386
이 정책 사용	2387
정책 세부 정보	2387
정책 버전	2387
JSON 정책 문서	2387
자세히 알아보기	2388
AWSQuickSightAssetBundleExportPolicy	2388
이 정책 사용	2388
정책 세부 정보	2388
정책 버전	2389
JSON 정책 문서	2389
자세히 알아보기	2391

AWSQuickSightAssetBundleImportPolicy	2391
이 정책 사용	2391
정책 세부 정보	2391
정책 버전	2391
JSON 정책 문서	2392
자세히 알아보기	2395
AWSQuickSightAthenaAccess	2395
이 정책 사용	2395
정책 세부 정보	2395
정책 버전	2395
JSON 정책 문서	2395
자세히 알아보기	2398
AWSQuickSightDescribeRDS	2398
이 정책 사용	2398
정책 세부 정보	2398
정책 버전	2398
JSON 정책 문서	2398
자세히 알아보기	2399
AWSQuickSightDescribeRedshift	2399
이 정책 사용	2399
정책 세부 정보	2399
정책 버전	2400
JSON 정책 문서	2400
자세히 알아보기	2400
AWSQuickSightElasticsearchPolicy	2400
이 정책 사용	2400
정책 세부 정보	2401
정책 버전	2401
JSON 정책 문서	2401
자세히 알아보기	2402
AWSQuickSightIoTAnalyticsAccess	2402
이 정책 사용	2402
정책 세부 정보	2403
정책 버전	2403
JSON 정책 문서	2403
자세히 알아보기	2403

AWSQuickSightListIAM	2404
이 정책 사용	2404
정책 세부 정보	2404
정책 버전	2404
JSON 정책 문서	2404
자세히 알아보기	2405
AWSQuicksightOpenSearchPolicy	2405
이 정책 사용	2405
정책 세부 정보	2405
정책 버전	2405
JSON 정책 문서	2405
자세히 알아보기	2406
AWSQuickSightSageMakerPolicy	2407
이 정책 사용	2407
정책 세부 정보	2407
정책 버전	2407
JSON 정책 문서	2407
자세히 알아보기	2409
AWSQuickSightTimestreamPolicy	2409
이 정책 사용	2409
정책 세부 정보	2409
정책 버전	2409
JSON 정책 문서	2409
자세히 알아보기	2410
AWSReachabilityAnalyzerServiceRolePolicy	2410
이 정책 사용	2410
정책 세부 정보	2411
정책 버전	2411
JSON 정책 문서	2411
자세히 알아보기	2413
AWSRefactoringToolkitFullAccess	2413
이 정책 사용	2414
정책 세부 정보	2414
정책 버전	2414
JSON 정책 문서	2414
자세히 알아보기	2428

AWSRefactoringToolkitSidecarPolicy	2428
이 정책 사용	2428
정책 세부 정보	2428
정책 버전	2428
JSON 정책 문서	2429
자세히 알아보기	2430
AWSrePostPrivateCloudWatchAccess	2430
이 정책 사용	2430
정책 세부 정보	2430
정책 버전	2430
JSON 정책 문서	2431
자세히 알아보기	2431
AWSRepostSpaceSupportOperationsPolicy	2431
이 정책 사용	2431
정책 세부 정보	2432
정책 버전	2432
JSON 정책 문서	2432
자세히 알아보기	2432
AWSResilienceHubAssessmentExecutionPolicy	2433
이 정책 사용	2433
정책 세부 정보	2433
정책 버전	2433
JSON 정책 문서	2433
자세히 알아보기	2437
AWSResourceAccessManagerFullAccess	2438
이 정책 사용	2438
정책 세부 정보	2438
정책 버전	2438
JSON 정책 문서	2438
자세히 알아보기	2439
AWSResourceAccessManagerReadOnlyAccess	2439
이 정책 사용	2439
정책 세부 정보	2439
정책 버전	2439
JSON 정책 문서	2440
자세히 알아보기	2440

AWSResourceAccessManagerResourceShareParticipantAccess	2440
이 정책 사용	2440
정책 세부 정보	2440
정책 버전	2441
JSON 정책 문서	2441
자세히 알아보기	2441
AWSResourceAccessManagerServiceRolePolicy	2442
이 정책 사용	2442
정책 세부 정보	2442
정책 버전	2442
JSON 정책 문서	2442
자세히 알아보기	2443
AWSResourceExplorerFullAccess	2443
이 정책 사용	2443
정책 세부 정보	2444
정책 버전	2444
JSON 정책 문서	2444
자세히 알아보기	2445
AWSResourceExplorerOrganizationsAccess	2445
이 정책 사용	2445
정책 세부 정보	2445
정책 버전	2446
JSON 정책 문서	2446
자세히 알아보기	2447
AWSResourceExplorerReadOnlyAccess	2448
이 정책 사용	2448
정책 세부 정보	2448
정책 버전	2448
JSON 정책 문서	2448
자세히 알아보기	2449
AWSResourceExplorerServiceRolePolicy	2449
이 정책 사용	2449
정책 세부 정보	2449
정책 버전	2450
JSON 정책 문서	2450
자세히 알아보기	2459

AWSResourceGroupsReadOnlyAccess	2459
이 정책 사용	2459
정책 세부 정보	2459
정책 버전	2459
JSON 정책 문서	2460
자세히 알아보기	2461
AWSRoboMaker_FullAccess	2461
이 정책 사용	2461
정책 세부 정보	2461
정책 버전	2462
JSON 정책 문서	2462
자세히 알아보기	2463
AWSRoboMakerReadOnlyAccess	2463
이 정책 사용	2463
정책 세부 정보	2463
정책 버전	2464
JSON 정책 문서	2464
자세히 알아보기	2464
AWSRoboMakerServicePolicy	2465
이 정책 사용	2465
정책 세부 정보	2465
정책 버전	2465
JSON 정책 문서	2465
자세히 알아보기	2467
AWSRoboMakerServiceRolePolicy	2467
이 정책 사용	2467
정책 세부 정보	2467
정책 버전	2467
JSON 정책 문서	2468
자세히 알아보기	2469
AWSRolesAnywhereServicePolicy	2469
이 정책 사용	2469
정책 세부 정보	2469
정책 버전	2469
JSON 정책 문서	2470
자세히 알아보기	2470

AWSS3OnOutpostsServiceRolePolicy	2471
이 정책 사용	2471
정책 세부 정보	2471
정책 버전	2471
JSON 정책 문서	2471
자세히 알아보기	2474
AWSSavingsPlansFullAccess	2474
이 정책 사용	2474
정책 세부 정보	2474
정책 버전	2474
JSON 정책 문서	2475
자세히 알아보기	2475
AWSSavingsPlansReadOnlyAccess	2475
이 정책 사용	2475
정책 세부 정보	2475
정책 버전	2476
JSON 정책 문서	2476
자세히 알아보기	2476
AWSSecurityHubFullAccess	2476
이 정책 사용	2477
정책 세부 정보	2477
정책 버전	2477
JSON 정책 문서	2477
자세히 알아보기	2478
AWSSecurityHubOrganizationsAccess	2478
이 정책 사용	2478
정책 세부 정보	2478
정책 버전	2479
JSON 정책 문서	2479
자세히 알아보기	2480
AWSSecurityHubReadOnlyAccess	2480
이 정책 사용	2480
정책 세부 정보	2480
정책 버전	2481
JSON 정책 문서	2481
자세히 알아보기	2481

AWSSecurityHubServiceRolePolicy	2481
이 정책 사용	2482
정책 세부 정보	2482
정책 버전	2482
JSON 정책 문서	2482
자세히 알아보기	2484
AWSServiceCatalogAdminFullAccess	2484
이 정책 사용	2484
정책 세부 정보	2484
정책 버전	2485
JSON 정책 문서	2485
자세히 알아보기	2488
AWSServiceCatalogAdminReadOnlyAccess	2488
이 정책 사용	2488
정책 세부 정보	2488
정책 버전	2488
JSON 정책 문서	2488
자세히 알아보기	2490
AWSServiceCatalogAppRegistryFullAccess	2490
이 정책 사용	2490
정책 세부 정보	2490
정책 버전	2490
JSON 정책 문서	2491
자세히 알아보기	2493
AWSServiceCatalogAppRegistryReadOnlyAccess	2493
이 정책 사용	2493
정책 세부 정보	2493
정책 버전	2493
JSON 정책 문서	2494
자세히 알아보기	2494
AWSServiceCatalogAppRegistryServiceRolePolicy	2494
이 정책 사용	2495
정책 세부 정보	2495
정책 버전	2495
JSON 정책 문서	2495
자세히 알아보기	2496

AWSServiceCatalogEndUserFullAccess	2497
이 정책 사용	2497
정책 세부 정보	2497
정책 버전	2497
JSON 정책 문서	2497
자세히 알아보기	2499
AWSServiceCatalogEndUserReadOnlyAccess	2499
이 정책 사용	2500
정책 세부 정보	2500
정책 버전	2500
JSON 정책 문서	2500
자세히 알아보기	2502
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	2502
이 정책 사용	2502
정책 세부 정보	2502
정책 버전	2502
JSON 정책 문서	2503
자세히 알아보기	2503
AWSServiceCatalogSyncServiceRolePolicy	2503
이 정책 사용	2503
정책 세부 정보	2504
정책 버전	2504
JSON 정책 문서	2504
자세히 알아보기	2505
AWSServiceRoleForAmazonEKSNodegroup	2505
이 정책 사용	2505
정책 세부 정보	2505
정책 버전	2506
JSON 정책 문서	2506
자세히 알아보기	2510
AWSServiceRoleForAmazonQDeveloper	2510
이 정책 사용	2510
정책 세부 정보	2510
정책 버전	2511
JSON 정책 문서	2511
자세히 알아보기	2511

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICEPOLICY	2511
이 정책 사용	2512
정책 세부 정보	2512
정책 버전	2512
JSON 정책 문서	2512
자세히 알아보기	2513
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsSERVICEPOLICY	2513
이 정책 사용	2513
정책 세부 정보	2513
정책 버전	2513
JSON 정책 문서	2513
자세히 알아보기	2514
AWSServiceRoleForCodeGuru-Profiler	2514
이 정책 사용	2514
정책 세부 정보	2514
정책 버전	2515
JSON 정책 문서	2515
자세히 알아보기	2515
AWSServiceRoleForCodeWhispererPolicy	2515
이 정책 사용	2516
정책 세부 정보	2516
정책 버전	2516
JSON 정책 문서	2516
자세히 알아보기	2518
AWSServiceRoleForEC2ScheduledInstances	2518
이 정책 사용	2518
정책 세부 정보	2518
정책 버전	2518
JSON 정책 문서	2519
자세히 알아보기	2520
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	2520
이 정책 사용	2520
정책 세부 정보	2520
정책 버전	2520
JSON 정책 문서	2520
자세히 알아보기	2521

AWSServiceRoleForImageBuilder	2521
이 정책 사용	2521
정책 세부 정보	2521
정책 버전	2522
JSON 정책 문서	2522
자세히 알아보기	2531
AWSServiceRoleForIoTSiteWise	2531
이 정책 사용	2532
정책 세부 정보	2532
정책 버전	2532
JSON 정책 문서	2532
자세히 알아보기	2534
AWSServiceRoleForLogDeliveryPolicy	2534
이 정책 사용	2534
정책 세부 정보	2534
정책 버전	2534
JSON 정책 문서	2534
자세히 알아보기	2535
AWSServiceRoleForMonitronPolicy	2535
이 정책 사용	2535
정책 세부 정보	2535
정책 버전	2536
JSON 정책 문서	2536
자세히 알아보기	2536
AWSServiceRoleForNeptuneGraphPolicy	2537
이 정책 사용	2537
정책 세부 정보	2537
정책 버전	2537
JSON 정책 문서	2537
자세히 알아보기	2539
AWSServiceRoleForPrivateMarketplaceAdminPolicy	2539
이 정책 사용	2539
정책 세부 정보	2539
정책 버전	2539
JSON 정책 문서	2539
자세히 알아보기	2541

AWSServiceRoleForSMS	2541
이 정책 사용	2541
정책 세부 정보	2541
정책 버전	2542
JSON 정책 문서	2542
자세히 알아보기	2549
AWSServiceRoleForUserSubscriptions	2549
이 정책 사용	2549
정책 세부 정보	2549
정책 버전	2549
JSON 정책 문서	2549
자세히 알아보기	2550
AWSServiceRolePolicyForBackupReports	2550
이 정책 사용	2550
정책 세부 정보	2550
정책 버전	2551
JSON 정책 문서	2551
자세히 알아보기	2552
AWSServiceRolePolicyForBackupRestoreTesting	2552
이 정책 사용	2552
정책 세부 정보	2553
정책 버전	2553
JSON 정책 문서	2553
자세히 알아보기	2556
AWSShieldDRTAcessPolicy	2556
이 정책 사용	2556
정책 세부 정보	2556
정책 버전	2556
JSON 정책 문서	2557
자세히 알아보기	2558
AWSShieldServiceRolePolicy	2558
이 정책 사용	2558
정책 세부 정보	2558
정책 버전	2558
JSON 정책 문서	2558
자세히 알아보기	2559

AWSSSMForSAPServiceLinkedRolePolicy	2559
이 정책 사용	2559
정책 세부 정보	2559
정책 버전	2560
JSON 정책 문서	2560
자세히 알아보기	2566
AWSSSMOpsInsightsServiceRolePolicy	2566
이 정책 사용	2567
정책 세부 정보	2567
정책 버전	2567
JSON 정책 문서	2567
자세히 알아보기	2568
AWSSSODirectoryAdministrator	2568
이 정책 사용	2568
정책 세부 정보	2568
정책 버전	2568
JSON 정책 문서	2569
자세히 알아보기	2569
AWSSSODirectoryReadOnly	2569
이 정책 사용	2569
정책 세부 정보	2570
정책 버전	2570
JSON 정책 문서	2570
자세히 알아보기	2571
AWSSSOMasterAccountAdministrator	2571
이 정책 사용	2571
정책 세부 정보	2571
정책 버전	2571
JSON 정책 문서	2571
자세히 알아보기	2573
AWSSSOMemberAccountAdministrator	2573
이 정책 사용	2574
정책 세부 정보	2574
정책 버전	2574
JSON 정책 문서	2574
자세히 알아보기	2575

AWSSSOReadOnly	2576
이 정책 사용	2576
정책 세부 정보	2576
정책 버전	2576
JSON 정책 문서	2576
자세히 알아보기	2577
AWSSSOServiceRolePolicy	2577
이 정책 사용	2577
정책 세부 정보	2578
정책 버전	2578
JSON 정책 문서	2578
자세히 알아보기	2581
AWSSStepFunctionsConsoleFullAccess	2582
이 정책 사용	2582
정책 세부 정보	2582
정책 버전	2582
JSON 정책 문서	2582
자세히 알아보기	2583
AWSSStepFunctionsFullAccess	2583
이 정책 사용	2583
정책 세부 정보	2583
정책 버전	2584
JSON 정책 문서	2584
자세히 알아보기	2584
AWSSStepFunctionsReadOnlyAccess	2584
이 정책 사용	2585
정책 세부 정보	2585
정책 버전	2585
JSON 정책 문서	2585
자세히 알아보기	2586
AWSSStorageGatewayFullAccess	2586
이 정책 사용	2586
정책 세부 정보	2586
정책 버전	2586
JSON 정책 문서	2587
자세히 알아보기	2587

AWSSStorageGatewayReadOnlyAccess	2588
이 정책 사용	2588
정책 세부 정보	2588
정책 버전	2588
JSON 정책 문서	2588
자세히 알아보기	2589
AWSSStorageGatewayServiceRolePolicy	2589
이 정책 사용	2589
정책 세부 정보	2589
정책 버전	2590
JSON 정책 문서	2590
자세히 알아보기	2590
AWSSupplyChainFederationAdminAccess	2590
이 정책 사용	2591
정책 세부 정보	2591
정책 버전	2591
JSON 정책 문서	2591
자세히 알아보기	2596
AWSSupportAccess	2597
이 정책 사용	2597
정책 세부 정보	2597
정책 버전	2597
JSON 정책 문서	2597
자세히 알아보기	2598
AWSSupportAppFullAccess	2598
이 정책 사용	2598
정책 세부 정보	2598
정책 버전	2598
JSON 정책 문서	2599
자세히 알아보기	2599
AWSSupportAppReadOnlyAccess	2600
이 정책 사용	2600
정책 세부 정보	2600
정책 버전	2600
JSON 정책 문서	2600
자세히 알아보기	2601

AWSSupportPlansFullAccess	2601
이 정책 사용	2601
정책 세부 정보	2601
정책 버전	2601
JSON 정책 문서	2601
자세히 알아보기	2602
AWSSupportPlansReadOnlyAccess	2602
이 정책 사용	2602
정책 세부 정보	2602
정책 버전	2603
JSON 정책 문서	2603
자세히 알아보기	2603
AWSSupportServiceRolePolicy	2603
이 정책 사용	2604
정책 세부 정보	2604
정책 버전	2604
JSON 정책 문서	2604
자세히 알아보기	2679
AWSSystemsManagerAccountDiscoveryServicePolicy	2680
이 정책 사용	2680
정책 세부 정보	2680
정책 버전	2680
JSON 정책 문서	2680
자세히 알아보기	2681
AWSSystemsManagerChangeManagementServicePolicy	2681
이 정책 사용	2681
정책 세부 정보	2681
정책 버전	2682
JSON 정책 문서	2682
자세히 알아보기	2683
AWSSystemsManagerForSAPFullAccess	2684
이 정책 사용	2684
정책 세부 정보	2684
정책 버전	2684
JSON 정책 문서	2684
자세히 알아보기	2685

AWSSystemsManagerForSAPReadOnlyAccess	2685
이 정책 사용	2685
정책 세부 정보	2685
정책 버전	2686
JSON 정책 문서	2686
자세히 알아보기	2686
AWSSystemsManagerOpsDataSyncServiceRolePolicy	2686
이 정책 사용	2687
정책 세부 정보	2687
정책 버전	2687
JSON 정책 문서	2687
자세히 알아보기	2691
AWSThinkboxAssetServerPolicy	2691
이 정책 사용	2691
정책 세부 정보	2691
정책 버전	2691
JSON 정책 문서	2691
자세히 알아보기	2692
AWSThinkboxAWSPortalAdminPolicy	2692
이 정책 사용	2693
정책 세부 정보	2693
정책 버전	2693
JSON 정책 문서	2693
자세히 알아보기	2703
AWSThinkboxAWSPortalGatewayPolicy	2703
이 정책 사용	2703
정책 세부 정보	2703
정책 버전	2704
JSON 정책 문서	2704
자세히 알아보기	2705
AWSThinkboxAWSPortalWorkerPolicy	2706
이 정책 사용	2706
정책 세부 정보	2706
정책 버전	2706
JSON 정책 문서	2706
자세히 알아보기	2708

AWSThinkboxDeadlineResourceTrackerAccessPolicy	2708
이 정책 사용	2709
정책 세부 정보	2709
정책 버전	2709
JSON 정책 문서	2709
자세히 알아보기	2712
AWSThinkboxDeadlineResourceTrackerAdminPolicy	2712
이 정책 사용	2712
정책 세부 정보	2712
정책 버전	2713
JSON 정책 문서	2713
자세히 알아보기	2719
AWSThinkboxDeadlineSpotEventPluginAdminPolicy	2719
이 정책 사용	2719
정책 세부 정보	2719
정책 버전	2719
JSON 정책 문서	2720
자세히 알아보기	2722
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	2723
이 정책 사용	2723
정책 세부 정보	2723
정책 버전	2723
JSON 정책 문서	2723
자세히 알아보기	2725
AWSTransferConsoleFullAccess	2725
이 정책 사용	2725
정책 세부 정보	2725
정책 버전	2725
JSON 정책 문서	2725
자세히 알아보기	2726
AWSTransferFullAccess	2727
이 정책 사용	2727
정책 세부 정보	2727
정책 버전	2727
JSON 정책 문서	2727
자세히 알아보기	2728

AWSTransferLoggingAccess	2728
이 정책 사용	2728
정책 세부 정보	2728
정책 버전	2729
JSON 정책 문서	2729
자세히 알아보기	2729
AWSTransferReadOnlyAccess	2730
이 정책 사용	2730
정책 세부 정보	2730
정책 버전	2730
JSON 정책 문서	2730
자세히 알아보기	2731
AWSTrustedAdvisorPriorityFullAccess	2731
이 정책 사용	2731
정책 세부 정보	2731
정책 버전	2731
JSON 정책 문서	2732
자세히 알아보기	2733
AWSTrustedAdvisorPriorityReadOnlyAccess	2734
이 정책 사용	2734
정책 세부 정보	2734
정책 버전	2734
JSON 정책 문서	2734
자세히 알아보기	2735
AWSTrustedAdvisorReportingServiceRolePolicy	2735
이 정책 사용	2736
정책 세부 정보	2736
정책 버전	2736
JSON 정책 문서	2736
자세히 알아보기	2737
AWSTrustedAdvisorServiceRolePolicy	2737
이 정책 사용	2737
정책 세부 정보	2737
정책 버전	2737
JSON 정책 문서	2738
자세히 알아보기	2740

AWSUserNotificationsServiceLinkedRolePolicy	2741
이 정책 사용	2741
정책 세부 정보	2741
정책 버전	2741
JSON 정책 문서	2741
자세히 알아보기	2742
AWSVendorInsightsAssessorFullAccess	2742
이 정책 사용	2742
정책 세부 정보	2742
정책 버전	2743
JSON 정책 문서	2743
자세히 알아보기	2744
AWSVendorInsightsAssessorReadOnly	2744
이 정책 사용	2744
정책 세부 정보	2744
정책 버전	2745
JSON 정책 문서	2745
자세히 알아보기	2745
AWSVendorInsightsVendorFullAccess	2746
이 정책 사용	2746
정책 세부 정보	2746
정책 버전	2746
JSON 정책 문서	2746
자세히 알아보기	2748
AWSVendorInsightsVendorReadOnly	2748
이 정책 사용	2748
정책 세부 정보	2748
정책 버전	2749
JSON 정책 문서	2749
자세히 알아보기	2750
AWSVpcLatticeServiceRolePolicy	2750
이 정책 사용	2750
정책 세부 정보	2750
정책 버전	2750
JSON 정책 문서	2751
자세히 알아보기	2751

AWSVPCS2SVpnServiceRolePolicy	2751
이 정책 사용	2751
정책 세부 정보	2752
정책 버전	2752
JSON 정책 문서	2752
자세히 알아보기	2752
AWSVPCTransitGatewayServiceRolePolicy	2753
이 정책 사용	2753
정책 세부 정보	2753
정책 버전	2753
JSON 정책 문서	2753
자세히 알아보기	2754
AWSVPCVerifiedAccessServiceRolePolicy	2754
이 정책 사용	2754
정책 세부 정보	2754
정책 버전	2755
JSON 정책 문서	2755
자세히 알아보기	2756
AWSWAFConsoleFullAccess	2756
이 정책 사용	2757
정책 세부 정보	2757
정책 버전	2757
JSON 정책 문서	2757
자세히 알아보기	2759
AWSWAFConsoleReadOnlyAccess	2759
이 정책 사용	2760
정책 세부 정보	2760
정책 버전	2760
JSON 정책 문서	2760
자세히 알아보기	2761
AWSWAFFullAccess	2761
이 정책 사용	2761
정책 세부 정보	2762
정책 버전	2762
JSON 정책 문서	2762
자세히 알아보기	2764

AWSWAFReadOnlyAccess	2764
이 정책 사용	2764
정책 세부 정보	2764
정책 버전	2764
JSON 정책 문서	2764
자세히 알아보기	2765
AWSWellArchitectedDiscoveryServiceRolePolicy	2765
이 정책 사용	2766
정책 세부 정보	2766
정책 버전	2766
JSON 정책 문서	2766
자세히 알아보기	2768
AWSWellArchitectedOrganizationsServiceRolePolicy	2768
이 정책 사용	2768
정책 세부 정보	2768
정책 버전	2768
JSON 정책 문서	2768
자세히 알아보기	2769
AWSWickrFullAccess	2769
이 정책 사용	2769
정책 세부 정보	2769
정책 버전	2770
JSON 정책 문서	2770
자세히 알아보기	2770
AWSXrayCrossAccountSharingConfiguration	2770
이 정책 사용	2770
정책 세부 정보	2771
정책 버전	2771
JSON 정책 문서	2771
자세히 알아보기	2772
AWSXRayDaemonWriteAccess	2772
이 정책 사용	2772
정책 세부 정보	2772
정책 버전	2773
JSON 정책 문서	2773
자세히 알아보기	2773

AWSXrayFullAccess	2773
이 정책 사용	2774
정책 세부 정보	2774
정책 버전	2774
JSON 정책 문서	2774
자세히 알아보기	2775
AWSXrayReadOnlyAccess	2775
이 정책 사용	2775
정책 세부 정보	2775
정책 버전	2775
JSON 정책 문서	2775
자세히 알아보기	2776
AWSXrayWriteOnlyAccess	2776
이 정책 사용	2777
정책 세부 정보	2777
정책 버전	2777
JSON 정책 문서	2777
자세히 알아보기	2778
AWSZonalAutoshiftPracticeRunSLRPolicy	2778
이 정책 사용	2778
정책 세부 정보	2778
정책 버전	2778
JSON 정책 문서	2779
자세히 알아보기	2779
BatchServiceRolePolicy	2779
이 정책 사용	2780
정책 세부 정보	2780
정책 버전	2780
JSON 정책 문서	2780
자세히 알아보기	2786
Billing	2786
이 정책 사용	2786
정책 세부 정보	2787
정책 버전	2787
JSON 정책 문서	2787
자세히 알아보기	2790

CertificateManagerServiceRolePolicy	2790
이 정책 사용	2790
정책 세부 정보	2790
정책 버전	2790
JSON 정책 문서	2791
자세히 알아보기	2791
ClientVPNServiceConnectionsRolePolicy	2791
이 정책 사용	2791
정책 세부 정보	2791
정책 버전	2792
JSON 정책 문서	2792
자세히 알아보기	2792
ClientVPNServiceRolePolicy	2792
이 정책 사용	2793
정책 세부 정보	2793
정책 버전	2793
JSON 정책 문서	2793
자세히 알아보기	2794
CloudFormationStackSetsOrgAdminServiceRolePolicy	2794
이 정책 사용	2794
정책 세부 정보	2794
정책 버전	2795
JSON 정책 문서	2795
자세히 알아보기	2795
CloudFormationStackSetsOrgMemberServiceRolePolicy	2795
이 정책 사용	2796
정책 세부 정보	2796
정책 버전	2796
JSON 정책 문서	2796
자세히 알아보기	2797
CloudFrontFullAccess	2797
이 정책 사용	2797
정책 세부 정보	2797
정책 버전	2798
JSON 정책 문서	2798
자세히 알아보기	2799

CloudFrontReadOnlyAccess	2799
이 정책 사용	2799
정책 세부 정보	2799
정책 버전	2800
JSON 정책 문서	2800
자세히 알아보기	2800
CloudHSMServiceRolePolicy	2801
이 정책 사용	2801
정책 세부 정보	2801
정책 버전	2801
JSON 정책 문서	2801
자세히 알아보기	2802
CloudSearchFullAccess	2802
이 정책 사용	2802
정책 세부 정보	2802
정책 버전	2802
JSON 정책 문서	2803
자세히 알아보기	2803
CloudSearchReadOnlyAccess	2803
이 정책 사용	2803
정책 세부 정보	2803
정책 버전	2804
JSON 정책 문서	2804
자세히 알아보기	2804
CloudTrailServiceRolePolicy	2804
이 정책 사용	2805
정책 세부 정보	2805
정책 버전	2805
JSON 정책 문서	2805
자세히 알아보기	2807
CloudWatch-CrossAccountAccess	2807
이 정책 사용	2807
정책 세부 정보	2807
정책 버전	2807
JSON 정책 문서	2808
자세히 알아보기	2808

CloudWatchActionsEC2Access	2808
이 정책 사용	2808
정책 세부 정보	2808
정책 버전	2809
JSON 정책 문서	2809
자세히 알아보기	2809
CloudWatchAgentAdminPolicy	2809
이 정책 사용	2810
정책 세부 정보	2810
정책 버전	2810
JSON 정책 문서	2810
자세히 알아보기	2811
CloudWatchAgentServerPolicy	2811
이 정책 사용	2811
정책 세부 정보	2811
정책 버전	2812
JSON 정책 문서	2812
자세히 알아보기	2813
CloudWatchApplicationInsightsFullAccess	2813
이 정책 사용	2813
정책 세부 정보	2813
정책 버전	2813
JSON 정책 문서	2814
자세히 알아보기	2815
CloudWatchApplicationInsightsReadOnlyAccess	2815
이 정책 사용	2815
정책 세부 정보	2815
정책 버전	2816
JSON 정책 문서	2816
자세히 알아보기	2816
CloudwatchApplicationInsightsServiceLinkedRolePolicy	2816
이 정책 사용	2817
정책 세부 정보	2817
정책 버전	2817
JSON 정책 문서	2817
자세히 알아보기	2827

CloudWatchApplicationSignalsFullAccess	2827
이 정책 사용	2827
정책 세부 정보	2827
정책 버전	2827
JSON 정책 문서	2828
자세히 알아보기	2830
CloudWatchApplicationSignalsReadOnlyAccess	2831
이 정책 사용	2831
정책 세부 정보	2831
정책 버전	2831
JSON 정책 문서	2831
자세히 알아보기	2833
CloudWatchApplicationSignalsServiceRolePolicy	2834
이 정책 사용	2834
정책 세부 정보	2834
정책 버전	2834
JSON 정책 문서	2834
자세히 알아보기	2837
CloudWatchAutomaticDashboardsAccess	2837
이 정책 사용	2837
정책 세부 정보	2837
정책 버전	2837
JSON 정책 문서	2837
자세히 알아보기	2839
CloudWatchCrossAccountSharingConfiguration	2839
이 정책 사용	2839
정책 세부 정보	2839
정책 버전	2839
JSON 정책 문서	2840
자세히 알아보기	2841
CloudWatchEventsBuiltInTargetExecutionAccess	2841
이 정책 사용	2841
정책 세부 정보	2841
정책 버전	2841
JSON 정책 문서	2842
자세히 알아보기	2842

CloudWatchEventsFullAccess	2842
이 정책 사용	2842
정책 세부 정보	2842
정책 버전	2843
JSON 정책 문서	2843
자세히 알아보기	2845
CloudWatchEventsInvocationAccess	2845
이 정책 사용	2845
정책 세부 정보	2845
정책 버전	2846
JSON 정책 문서	2846
자세히 알아보기	2846
CloudWatchEventsReadOnlyAccess	2846
이 정책 사용	2846
정책 세부 정보	2847
정책 버전	2847
JSON 정책 문서	2847
자세히 알아보기	2848
CloudWatchEventsServiceRolePolicy	2848
이 정책 사용	2849
정책 세부 정보	2849
정책 버전	2849
JSON 정책 문서	2849
자세히 알아보기	2850
CloudWatchFullAccess	2850
이 정책 사용	2850
정책 세부 정보	2850
정책 버전	2850
JSON 정책 문서	2851
자세히 알아보기	2852
CloudWatchFullAccessV2	2852
이 정책 사용	2852
정책 세부 정보	2852
정책 버전	2852
JSON 정책 문서	2852
자세히 알아보기	2854

CloudWatchInternetMonitorServiceRolePolicy	2854
이 정책 사용	2854
정책 세부 정보	2854
정책 버전	2855
JSON 정책 문서	2855
자세히 알아보기	2856
CloudWatchLambdaInsightsExecutionRolePolicy	2856
이 정책 사용	2856
정책 세부 정보	2856
정책 버전	2856
JSON 정책 문서	2857
자세히 알아보기	2857
CloudWatchLogsCrossAccountSharingConfiguration	2857
이 정책 사용	2858
정책 세부 정보	2858
정책 버전	2858
JSON 정책 문서	2858
자세히 알아보기	2859
CloudWatchLogsFullAccess	2859
이 정책 사용	2859
정책 세부 정보	2859
정책 버전	2860
JSON 정책 문서	2860
자세히 알아보기	2860
CloudWatchLogsReadOnlyAccess	2860
이 정책 사용	2861
정책 세부 정보	2861
정책 버전	2861
JSON 정책 문서	2861
자세히 알아보기	2862
CloudWatchNetworkMonitorServiceRolePolicy	2862
이 정책 사용	2862
정책 세부 정보	2862
정책 버전	2862
JSON 정책 문서	2863
자세히 알아보기	2864

CloudWatchReadOnlyAccess	2864
이 정책 사용	2864
정책 세부 정보	2864
정책 버전	2865
JSON 정책 문서	2865
자세히 알아보기	2866
CloudWatchSyntheticsFullAccess	2866
이 정책 사용	2866
정책 세부 정보	2867
정책 버전	2867
JSON 정책 문서	2867
자세히 알아보기	2872
CloudWatchSyntheticsReadOnlyAccess	2872
이 정책 사용	2872
정책 세부 정보	2872
정책 버전	2872
JSON 정책 문서	2872
자세히 알아보기	2873
ComprehendDataAccessRolePolicy	2873
이 정책 사용	2873
정책 세부 정보	2873
정책 버전	2874
JSON 정책 문서	2874
자세히 알아보기	2874
ComprehendFullAccess	2874
이 정책 사용	2875
정책 세부 정보	2875
정책 버전	2875
JSON 정책 문서	2875
자세히 알아보기	2876
ComprehendMedicalFullAccess	2876
이 정책 사용	2876
정책 세부 정보	2876
정책 버전	2876
JSON 정책 문서	2876
자세히 알아보기	2877

ComprehendReadOnly	2877
이 정책 사용	2877
정책 세부 정보	2877
정책 버전	2877
JSON 정책 문서	2878
자세히 알아보기	2879
ComputeOptimizerReadOnlyAccess	2879
이 정책 사용	2879
정책 세부 정보	2879
정책 버전	2880
JSON 정책 문서	2880
자세히 알아보기	2881
ComputeOptimizerServiceRolePolicy	2881
이 정책 사용	2881
정책 세부 정보	2881
정책 버전	2881
JSON 정책 문서	2882
자세히 알아보기	2883
ConfigConformsServiceRolePolicy	2883
이 정책 사용	2883
정책 세부 정보	2883
정책 버전	2884
JSON 정책 문서	2884
자세히 알아보기	2886
CostOptimizationHubAdminAccess	2887
이 정책 사용	2887
정책 세부 정보	2887
정책 버전	2887
JSON 정책 문서	2887
자세히 알아보기	2889
CostOptimizationHubReadOnlyAccess	2889
이 정책 사용	2889
정책 세부 정보	2889
정책 버전	2889
JSON 정책 문서	2889
자세히 알아보기	2890

CostOptimizationHubServiceRolePolicy	2890
이 정책 사용	2890
정책 세부 정보	2890
정책 버전	2891
JSON 정책 문서	2891
자세히 알아보기	2892
CustomerProfilesServiceLinkedRolePolicy	2892
이 정책 사용	2892
정책 세부 정보	2892
정책 버전	2892
JSON 정책 문서	2893
자세히 알아보기	2893
DatabaseAdministrator	2893
이 정책 사용	2894
정책 세부 정보	2894
정책 버전	2894
JSON 정책 문서	2894
자세히 알아보기	2896
DataScientist	2897
이 정책 사용	2897
정책 세부 정보	2897
정책 버전	2897
JSON 정책 문서	2897
자세히 알아보기	2901
DAXServiceRolePolicy	2901
이 정책 사용	2901
정책 세부 정보	2901
정책 버전	2902
JSON 정책 문서	2902
자세히 알아보기	2902
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	2903
이 정책 사용	2903
정책 세부 정보	2903
정책 버전	2903
JSON 정책 문서	2903
자세히 알아보기	2904

DynamoDBKinesisReplicationServiceRolePolicy	2904
이 정책 사용	2904
정책 세부 정보	2904
정책 버전	2905
JSON 정책 문서	2905
자세히 알아보기	2905
DynamoDBReplicationServiceRolePolicy	2906
이 정책 사용	2906
정책 세부 정보	2906
정책 버전	2906
JSON 정책 문서	2906
자세히 알아보기	2907
EC2FastLaunchFullAccess	2908
이 정책 사용	2908
정책 세부 정보	2908
정책 버전	2908
JSON 정책 문서	2908
자세히 알아보기	2911
EC2FastLaunchServiceRolePolicy	2911
이 정책 사용	2911
정책 세부 정보	2911
정책 버전	2912
JSON 정책 문서	2912
자세히 알아보기	2916
EC2FleetTimeShiftableServiceRolePolicy	2916
이 정책 사용	2916
정책 세부 정보	2916
정책 버전	2916
JSON 정책 문서	2916
자세히 알아보기	2918
Ec2ImageBuilderCrossAccountDistributionAccess	2918
이 정책 사용	2918
정책 세부 정보	2918
정책 버전	2918
JSON 정책 문서	2919
자세히 알아보기	2919

EC2ImageBuilderLifecycleExecutionPolicy	2919
이 정책 사용	2920
정책 세부 정보	2920
정책 버전	2920
JSON 정책 문서	2920
자세히 알아보기	2922
EC2InstanceConnect	2922
이 정책 사용	2922
정책 세부 정보	2923
정책 버전	2923
JSON 정책 문서	2923
자세히 알아보기	2923
Ec2InstanceConnectEndpoint	2924
이 정책 사용	2924
정책 세부 정보	2924
정책 버전	2924
JSON 정책 문서	2924
자세히 알아보기	2926
EC2InstanceProfileForImageBuilder	2926
이 정책 사용	2927
정책 세부 정보	2927
정책 버전	2927
JSON 정책 문서	2927
자세히 알아보기	2928
EC2InstanceProfileForImageBuilderECRContainerBuilds	2928
이 정책 사용	2929
정책 세부 정보	2929
정책 버전	2929
JSON 정책 문서	2929
자세히 알아보기	2930
ECRReplicationServiceRolePolicy	2931
이 정책 사용	2931
정책 세부 정보	2931
정책 버전	2931
JSON 정책 문서	2931
자세히 알아보기	2932

ElastiCacheServiceRolePolicy	2932
이 정책 사용	2932
정책 세부 정보	2932
정책 버전	2932
JSON 정책 문서	2933
자세히 알아보기	2934
ElasticLoadBalancingFullAccess	2935
이 정책 사용	2935
정책 세부 정보	2935
정책 버전	2935
JSON 정책 문서	2935
자세히 알아보기	2937
ElasticLoadBalancingReadOnly	2937
이 정책 사용	2937
정책 세부 정보	2937
정책 버전	2937
JSON 정책 문서	2937
자세히 알아보기	2938
ElementalActivationsDownloadSoftwareAccess	2939
이 정책 사용	2939
정책 세부 정보	2939
정책 버전	2939
JSON 정책 문서	2939
자세히 알아보기	2940
ElementalActivationsFullAccess	2940
이 정책 사용	2940
정책 세부 정보	2940
정책 버전	2940
JSON 정책 문서	2941
자세히 알아보기	2941
ElementalActivationsGenerateLicenses	2941
이 정책 사용	2941
정책 세부 정보	2941
정책 버전	2942
JSON 정책 문서	2942
자세히 알아보기	2942

ElementalActivationsReadOnlyAccess	2942
이 정책 사용	2943
정책 세부 정보	2943
정책 버전	2943
JSON 정책 문서	2943
자세히 알아보기	2943
ElementalAppliancesSoftwareFullAccess	2944
이 정책 사용	2944
정책 세부 정보	2944
정책 버전	2944
JSON 정책 문서	2944
자세히 알아보기	2945
ElementalAppliancesSoftwareReadOnlyAccess	2945
이 정책 사용	2945
정책 세부 정보	2945
정책 버전	2945
JSON 정책 문서	2946
자세히 알아보기	2946
ElementalSupportCenterFullAccess	2946
이 정책 사용	2946
정책 세부 정보	2946
정책 버전	2947
JSON 정책 문서	2947
자세히 알아보기	2947
EMRDescribeClusterPolicyForEMRWAL	2947
이 정책 사용	2948
정책 세부 정보	2948
정책 버전	2948
JSON 정책 문서	2948
자세히 알아보기	2949
FMSServiceRolePolicy	2949
이 정책 사용	2949
정책 세부 정보	2949
정책 버전	2949
JSON 정책 문서	2949
자세히 알아보기	2965

FSxDeleteServiceLinkedRoleAccess	2966
이 정책 사용	2966
정책 세부 정보	2966
정책 버전	2966
JSON 정책 문서	2966
자세히 알아보기	2967
GameLiftGameServerGroupPolicy	2967
이 정책 사용	2967
정책 세부 정보	2967
정책 버전	2967
JSON 정책 문서	2968
자세히 알아보기	2969
GlobalAcceleratorFullAccess	2969
이 정책 사용	2969
정책 세부 정보	2970
정책 버전	2970
JSON 정책 문서	2970
자세히 알아보기	2971
GlobalAcceleratorReadOnlyAccess	2971
이 정책 사용	2971
정책 세부 정보	2971
정책 버전	2972
JSON 정책 문서	2972
자세히 알아보기	2972
GreengrassOTAUpdateArtifactAccess	2972
이 정책 사용	2973
정책 세부 정보	2973
정책 버전	2973
JSON 정책 문서	2973
자세히 알아보기	2974
GroundTruthSyntheticConsoleFullAccess	2974
이 정책 사용	2974
정책 세부 정보	2974
정책 버전	2974
JSON 정책 문서	2974
자세히 알아보기	2975

GroundTruthSyntheticConsoleReadOnlyAccess	2975
이 정책 사용	2975
정책 세부 정보	2975
정책 버전	2976
JSON 정책 문서	2976
자세히 알아보기	2976
Health_OrganizationsServiceRolePolicy	2976
이 정책 사용	2977
정책 세부 정보	2977
정책 버전	2977
JSON 정책 문서	2977
자세히 알아보기	2978
IAMAccessAdvisorReadOnly	2978
이 정책 사용	2978
정책 세부 정보	2978
정책 버전	2978
JSON 정책 문서	2978
자세히 알아보기	2979
IAMAccessAnalyzerFullAccess	2980
이 정책 사용	2980
정책 세부 정보	2980
정책 버전	2980
JSON 정책 문서	2980
자세히 알아보기	2981
IAMAccessAnalyzerReadOnlyAccess	2981
이 정책 사용	2982
정책 세부 정보	2982
정책 버전	2982
JSON 정책 문서	2982
자세히 알아보기	2983
IAMFullAccess	2983
이 정책 사용	2983
정책 세부 정보	2983
정책 버전	2983
JSON 정책 문서	2983
자세히 알아보기	2984

IAMReadOnlyAccess	2984
이 정책 사용	2984
정책 세부 정보	2984
정책 버전	2985
JSON 정책 문서	2985
자세히 알아보기	2985
IAMSelfManageServiceSpecificCredentials	2986
이 정책 사용	2986
정책 세부 정보	2986
정책 버전	2986
JSON 정책 문서	2986
자세히 알아보기	2987
IAMUserChangePassword	2987
이 정책 사용	2987
정책 세부 정보	2987
정책 버전	2987
JSON 정책 문서	2988
자세히 알아보기	2988
IAMUserSSHKeys	2988
이 정책 사용	2988
정책 세부 정보	2989
정책 버전	2989
JSON 정책 문서	2989
자세히 알아보기	2989
IVSFullAccess	2990
이 정책 사용	2990
정책 세부 정보	2990
정책 버전	2990
JSON 정책 문서	2990
자세히 알아보기	2991
IVSReadOnlyAccess	2991
이 정책 사용	2991
정책 세부 정보	2991
정책 버전	2991
JSON 정책 문서	2992
자세히 알아보기	2993

IVSRecordToS3	2993
이 정책 사용	2993
정책 세부 정보	2993
정책 버전	2993
JSON 정책 문서	2994
자세히 알아보기	2994
KafkaConnectServiceRolePolicy	2994
이 정책 사용	2994
정책 세부 정보	2994
정책 버전	2995
JSON 정책 문서	2995
자세히 알아보기	2996
KafkaServiceRolePolicy	2996
이 정책 사용	2997
정책 세부 정보	2997
정책 버전	2997
JSON 정책 문서	2997
자세히 알아보기	2999
KeyspacesReplicationServiceRolePolicy	2999
이 정책 사용	2999
정책 세부 정보	2999
정책 버전	2999
JSON 정책 문서	2999
자세히 알아보기	3000
LakeFormationDataAccessServiceRolePolicy	3000
이 정책 사용	3000
정책 세부 정보	3000
정책 버전	3001
JSON 정책 문서	3001
자세히 알아보기	3001
LexBotPolicy	3001
이 정책 사용	3002
정책 세부 정보	3002
정책 버전	3002
JSON 정책 문서	3002
자세히 알아보기	3003

LexChannelPolicy	3003
이 정책 사용	3003
정책 세부 정보	3003
정책 버전	3003
JSON 정책 문서	3004
자세히 알아보기	3004
LightsailExportAccess	3004
이 정책 사용	3004
정책 세부 정보	3004
정책 버전	3005
JSON 정책 문서	3005
자세히 알아보기	3006
MediaConnectGatewayInstanceRolePolicy	3006
이 정책 사용	3006
정책 세부 정보	3006
정책 버전	3006
JSON 정책 문서	3006
자세히 알아보기	3007
MediaPackageServiceRolePolicy	3007
이 정책 사용	3007
정책 세부 정보	3007
정책 버전	3008
JSON 정책 문서	3008
자세히 알아보기	3008
MemoryDBServiceRolePolicy	3008
이 정책 사용	3009
정책 세부 정보	3009
정책 버전	3009
JSON 정책 문서	3009
자세히 알아보기	3011
MigrationHubDMSAccessServiceRolePolicy	3011
이 정책 사용	3011
정책 세부 정보	3011
정책 버전	3012
JSON 정책 문서	3012
자세히 알아보기	3013

MigrationHubServiceRolePolicy	3013
이 정책 사용	3013
정책 세부 정보	3013
정책 버전	3013
JSON 정책 문서	3014
자세히 알아보기	3015
MigrationHubSMSAccessServiceRolePolicy	3015
이 정책 사용	3015
정책 세부 정보	3015
정책 버전	3016
JSON 정책 문서	3016
자세히 알아보기	3017
MonitronServiceRolePolicy	3017
이 정책 사용	3017
정책 세부 정보	3017
정책 버전	3017
JSON 정책 문서	3018
자세히 알아보기	3018
NeptuneConsoleFullAccess	3018
이 정책 사용	3018
정책 세부 정보	3019
정책 버전	3019
JSON 정책 문서	3019
자세히 알아보기	3024
NeptuneFullAccess	3025
이 정책 사용	3025
정책 세부 정보	3025
정책 버전	3025
JSON 정책 문서	3025
자세히 알아보기	3029
NeptuneGraphReadOnlyAccess	3029
이 정책 사용	3030
정책 세부 정보	3030
정책 버전	3030
JSON 정책 문서	3030
자세히 알아보기	3032

NeptuneReadOnlyAccess	3032
이 정책 사용	3032
정책 세부 정보	3032
정책 버전	3032
JSON 정책 문서	3032
자세히 알아보기	3035
NetworkAdministrator	3035
이 정책 사용	3035
정책 세부 정보	3035
정책 버전	3035
JSON 정책 문서	3036
자세히 알아보기	3042
OAMFullAccess	3042
이 정책 사용	3042
정책 세부 정보	3043
정책 버전	3043
JSON 정책 문서	3043
자세히 알아보기	3043
OAMReadOnlyAccess	3044
이 정책 사용	3044
정책 세부 정보	3044
정책 버전	3044
JSON 정책 문서	3044
자세히 알아보기	3045
OpensearchIngestionSelfManagedVpcePolicy	3045
이 정책 사용	3045
정책 세부 정보	3045
정책 버전	3045
JSON 정책 문서	3046
자세히 알아보기	3046
PartnerCentralAccountManagementUserRoleAssociation	3046
이 정책 사용	3047
정책 세부 정보	3047
정책 버전	3047
JSON 정책 문서	3047
자세히 알아보기	3048

PowerUserAccess	3048
이 정책 사용	3048
정책 세부 정보	3048
정책 버전	3049
JSON 정책 문서	3049
자세히 알아보기	3049
QBusinessServiceRolePolicy	3050
이 정책 사용	3050
정책 세부 정보	3050
정책 버전	3050
JSON 정책 문서	3050
자세히 알아보기	3052
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	3052
이 정책 사용	3052
정책 세부 정보	3052
정책 버전	3053
JSON 정책 문서	3053
자세히 알아보기	3053
RDSCloudHsmAuthorizationRole	3054
이 정책 사용	3054
정책 세부 정보	3054
정책 버전	3054
JSON 정책 문서	3054
자세히 알아보기	3055
ReadOnlyAccess	3055
이 정책 사용	3055
정책 세부 정보	3055
정책 버전	3055
JSON 정책 문서	3056
자세히 알아보기	3105
ResourceGroupsandTagEditorFullAccess	3105
이 정책 사용	3105
정책 세부 정보	3105
정책 버전	3106
JSON 정책 문서	3106
자세히 알아보기	3106

ResourceGroupsandTagEditorReadOnlyAccess	3107
이 정책 사용	3107
정책 세부 정보	3107
정책 버전	3107
JSON 정책 문서	3107
자세히 알아보기	3108
ResourceGroupsServiceRolePolicy	3108
이 정책 사용	3108
정책 세부 정보	3108
정책 버전	3109
JSON 정책 문서	3109
자세히 알아보기	3109
ROSAAmazonEBSCSIDriverOperatorPolicy	3109
이 정책 사용	3110
정책 세부 정보	3110
정책 버전	3110
JSON 정책 문서	3110
자세히 알아보기	3113
ROSACloudNetworkConfigOperatorPolicy	3113
이 정책 사용	3113
정책 세부 정보	3114
정책 버전	3114
JSON 정책 문서	3114
자세히 알아보기	3115
ROSAControlPlaneOperatorPolicy	3115
이 정책 사용	3115
정책 세부 정보	3115
정책 버전	3116
JSON 정책 문서	3116
자세히 알아보기	3120
ROSAImageRegistryOperatorPolicy	3120
이 정책 사용	3121
정책 세부 정보	3121
정책 버전	3121
JSON 정책 문서	3121
자세히 알아보기	3122

ROSAIngressOperatorPolicy	3123
이 정책 사용	3123
정책 세부 정보	3123
정책 버전	3123
JSON 정책 문서	3123
자세히 알아보기	3124
ROSAInstallerPolicy	3124
이 정책 사용	3124
정책 세부 정보	3125
정책 버전	3125
JSON 정책 문서	3125
자세히 알아보기	3133
ROSAKMSProviderPolicy	3133
이 정책 사용	3133
정책 세부 정보	3133
정책 버전	3134
JSON 정책 문서	3134
자세히 알아보기	3134
ROSAKubeControllerPolicy	3135
이 정책 사용	3135
정책 세부 정보	3135
정책 버전	3135
JSON 정책 문서	3135
자세히 알아보기	3140
ROSAManageSubscription	3140
이 정책 사용	3140
정책 세부 정보	3140
정책 버전	3140
JSON 정책 문서	3140
자세히 알아보기	3141
ROSANodePoolManagementPolicy	3141
이 정책 사용	3142
정책 세부 정보	3142
정책 버전	3142
JSON 정책 문서	3142
자세히 알아보기	3148

ROSASRESupportPolicy	3148
이 정책 사용	3148
정책 세부 정보	3148
정책 버전	3148
JSON 정책 문서	3149
자세히 알아보기	3153
ROSAWorkerInstancePolicy	3154
이 정책 사용	3154
정책 세부 정보	3154
정책 버전	3154
JSON 정책 문서	3154
자세히 알아보기	3155
Route53RecoveryReadinessServiceRolePolicy	3155
이 정책 사용	3155
정책 세부 정보	3155
정책 버전	3155
JSON 정책 문서	3156
자세히 알아보기	3159
Route53ResolverServiceRolePolicy	3159
이 정책 사용	3159
정책 세부 정보	3159
정책 버전	3160
JSON 정책 문서	3160
자세히 알아보기	3160
S3StorageLensServiceRolePolicy	3161
이 정책 사용	3161
정책 세부 정보	3161
정책 버전	3161
JSON 정책 문서	3161
자세히 알아보기	3162
SecretsManagerReadWrite	3162
이 정책 사용	3162
정책 세부 정보	3162
정책 버전	3162
JSON 정책 문서	3163
자세히 알아보기	3164

SecurityAudit	3164
이 정책 사용	3165
정책 세부 정보	3165
정책 버전	3165
JSON 정책 문서	3165
자세히 알아보기	3182
SecurityLakeServiceLinkedRole	3183
이 정책 사용	3183
정책 세부 정보	3183
정책 버전	3183
JSON 정책 문서	3183
자세히 알아보기	3186
ServerMigration_ServiceRole	3186
이 정책 사용	3186
정책 세부 정보	3186
정책 버전	3187
JSON 정책 문서	3187
자세히 알아보기	3192
ServerMigrationConnector	3192
이 정책 사용	3192
정책 세부 정보	3192
정책 버전	3192
JSON 정책 문서	3193
자세히 알아보기	3194
ServerMigrationServiceConsoleFullAccess	3194
이 정책 사용	3194
정책 세부 정보	3194
정책 버전	3195
JSON 정책 문서	3195
자세히 알아보기	3196
ServerMigrationServiceLaunchRole	3197
이 정책 사용	3197
정책 세부 정보	3197
정책 버전	3197
JSON 정책 문서	3197
자세히 알아보기	3200

ServerMigrationServiceRoleForInstanceValidation	3200
이 정책 사용	3200
정책 세부 정보	3201
정책 버전	3201
JSON 정책 문서	3201
자세히 알아보기	3201
ServiceQuotasFullAccess	3202
이 정책 사용	3202
정책 세부 정보	3202
정책 버전	3202
JSON 정책 문서	3202
자세히 알아보기	3204
ServiceQuotasReadOnlyAccess	3204
이 정책 사용	3204
정책 세부 정보	3204
정책 버전	3205
JSON 정책 문서	3205
자세히 알아보기	3206
ServiceQuotasServiceRolePolicy	3206
이 정책 사용	3206
정책 세부 정보	3206
정책 버전	3206
JSON 정책 문서	3207
자세히 알아보기	3207
SimpleWorkflowFullAccess	3207
이 정책 사용	3207
정책 세부 정보	3207
정책 버전	3208
JSON 정책 문서	3208
자세히 알아보기	3208
SplitCostAllocationDataServiceRolePolicy	3208
이 정책 사용	3209
정책 세부 정보	3209
정책 버전	3209
JSON 정책 문서	3209
자세히 알아보기	3210

SupportUser	3210
이 정책 사용	3210
정책 세부 정보	3210
정책 버전	3210
JSON 정책 문서	3211
자세히 알아보기	3216
SystemAdministrator	3216
이 정책 사용	3216
정책 세부 정보	3216
정책 버전	3216
JSON 정책 문서	3216
자세히 알아보기	3222
TranslateFullAccess	3223
이 정책 사용	3223
정책 세부 정보	3223
정책 버전	3223
JSON 정책 문서	3223
자세히 알아보기	3224
TranslateReadOnly	3224
이 정책 사용	3224
정책 세부 정보	3224
정책 버전	3224
JSON 정책 문서	3225
자세히 알아보기	3225
ViewOnlyAccess	3225
이 정책 사용	3226
정책 세부 정보	3226
정책 버전	3226
JSON 정책 문서	3226
자세히 알아보기	3235
VMImportExportRoleForAWSConnector	3235
이 정책 사용	3235
정책 세부 정보	3235
정책 버전	3235
JSON 정책 문서	3236
자세히 알아보기	3236

VPCLatticeFullAccess	3236
이 정책 사용	3237
정책 세부 정보	3237
정책 버전	3237
JSON 정책 문서	3237
자세히 알아보기	3239
VPCLatticeReadOnlyAccess	3239
이 정책 사용	3239
정책 세부 정보	3240
정책 버전	3240
JSON 정책 문서	3240
자세히 알아보기	3241
VPCLatticeServicesInvokeAccess	3241
이 정책 사용	3241
정책 세부 정보	3241
정책 버전	3241
JSON 정책 문서	3242
자세히 알아보기	3242
WAFLoggingServiceRolePolicy	3242
이 정책 사용	3242
정책 세부 정보	3243
정책 버전	3243
JSON 정책 문서	3243
자세히 알아보기	3243
WAFRegionalLoggingServiceRolePolicy	3244
이 정책 사용	3244
정책 세부 정보	3244
정책 버전	3244
JSON 정책 문서	3244
자세히 알아보기	3245
WAFV2LoggingServiceRolePolicy	3245
이 정책 사용	3245
정책 세부 정보	3245
정책 버전	3245
JSON 정책 문서	3246
자세히 알아보기	3246

WellArchitectedConsoleFullAccess	3246
이 정책 사용	3246
정책 세부 정보	3247
정책 버전	3247
JSON 정책 문서	3247
자세히 알아보기	3247
WellArchitectedConsoleReadOnlyAccess	3248
이 정책 사용	3248
정책 세부 정보	3248
정책 버전	3248
JSON 정책 문서	3248
자세히 알아보기	3249
WorkLinkServiceRolePolicy	3249
이 정책 사용	3249
정책 세부 정보	3249
정책 버전	3249
JSON 정책 문서	3250
자세히 알아보기	3250
.....	mmmccli

AWS 관리형 정책이란 무엇인가요?

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다. 이를 사용하면 직접 정책을 작성하는 경우보다는 사용자, 그룹 및 역할에 권한 할당을 시작하는 것이 더욱 쉽습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#)을 참조하세요.

정책 참조 페이지 이해

각 정책 참조 페이지에는 다음 정보가 포함됩니다.

- 이 정책 사용 - 사용자, 그룹, 역할에 정책을 연결할 수 있는지 여부
- 정책 세부 정보
 - 유형 - AWS 관리형 정책 유형
 - AWS managed policy - 표준 AWS 관리형 정책
 - Job function policy - 업계 공통 직무 기능에 부합하는 정책
 - Service-linked role policy - 서비스가 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결된 정책(예: [the section called “AmazonRDSPreviewServiceRolePolicy”](#))
 - Service role policy - 서비스 역할과 연계되도록 설계된 정책(예: [the section called “AWSControlTowerServiceRolePolicy”](#))
 - 생성 시간 - 정책이 처음 생성된 시점
 - 편집된 시간 - 이 버전의 정책이 편집된 시점
 - ARN - 정책의 Amazon 리소스 이름(ARN)
- 정책 버전 - 정책에 의해 부여된 권한의 버전
- JSON 정책 문서 - 정책 JSON

- 자세히 알아보기 - AWS 관리형 정책과 관련된 설명서 링크

사용되지 않는 AWS 관리형 정책

AWS는 AWS 관리형 정책을 정기적으로 업데이트합니다. 대부분의 경우, 정책에 권한을 추가합니다. 이는 새 서비스나 기능을 출시할 때 발생합니다. AWS 관리형 정책의 보안을 개선하기 위해 때때로 정책 범위를 축소합니다. 정책에서 권한을 제거할 때는 정책을 사용 중단 상태로 설정하고 새 정책을 사용할 수 있도록 만듭니다. AWS가 서비스 또는 기능을 더 이상 사용하지 않는 경우 해당 기능에 대한 AWS 관리형 정책도 더 이상 사용되지 않습니다.

사용 중인 정책이 더 이상 사용되지 않는다는 이메일 알림을 받으면 즉시 조치를 취하는 것이 좋습니다. 정책 변경 사항을 파악하고 워크플로를 업데이트하세요. AWS가 대체 정책을 제공하는 경우 영향을 받는 모든 자격 증명(사용자, 그룹 및 역할)에 이를 연결한 다음 해당 자격 증명에서 더 이상 사용되지 않는 정책을 분리할 계획입니다.

사용되지 않는 정책은 다음과 같은 특성을 갖습니다.

- 이 안내서에서는 삭제되었습니다.
- 권한은 현재 연결된 모든 자격 증명에 대해 계속 작동합니다.
- 정책이 자격 증명에 연결된 계정에서는 IAM 콘솔의 정책 목록에 경고 아이콘과 함께 표시됩니다.
- 새 자격 증명에는 연결할 수 없습니다. 현재 자격 증명에서 연결을 해제할 경우 다시 연결할 수 없습니다.
- 현재의 모든 엔터티로부터 연결을 해제하면 더 이상 표시되지 않습니다.

AWS 관리형 정책

AWS 관리형 정책

- [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](#)
- [AmazonEKSConectorServiceRolePolicy](#)
- [AmazonEKSFargatePodExecutionRolePolicy](#)
- [AmazonEKSFargateServiceRolePolicy](#)
- [AmazonEKSLocalOutpostClusterPolicy](#)
- [AmazonEKSLocalOutpostServiceRolePolicy](#)
- [AmazonEKSServicePolicy](#)
- [AmazonEKSServiceRolePolicy](#)
- [AmazonEKSVPCResourceController](#)
- [AmazonEKSWorkerNodePolicy](#)
- [AmazonElastiCacheFullAccess](#)

- [AmazonElasticCacheReadOnlyAccess](#)
- [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](#)
- [AWElasticBeanstalkCustomPlatformforEC2Role](#)
- [AWElasticBeanstalkEnhancedHealth](#)
- [AWElasticBeanstalkMaintenance](#)

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

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

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

- [AWSImageBuilderReadOnlyAccess](#)
- [AWSImportExportFullAccess](#)
- [AWSImportExportReadOnlyAccess](#)
- [AWSIncidentManagerIncidentAccessServiceRolePolicy](#)
- [AWSIncidentManagerResolverAccess](#)
- [AWSIncidentManagerServiceRolePolicy](#)
- [AWSIoTClickFullAccess](#)
- [AWSIoTClickReadOnlyAccess](#)
- [AWSIoTAnalyticsFullAccess](#)
- [AWSIoTAnalyticsReadOnlyAccess](#)
- [AWSIoTConfigAccess](#)
- [AWSIoTConfigReadOnlyAccess](#)
- [AWSIoTDataAccess](#)
- [AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction](#)
- [AWSIoTDeviceDefenderAudit](#)
- [AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction](#)
- [AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction](#)
- [AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateCACertMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction](#)
- [AWSIoTDeviceTesterForFreeRTOSFullAccess](#)
- [AWSIoTDeviceTesterForGreengrassFullAccess](#)
- [AWSIOTEventsFullAccess](#)
- [AWSIOTEventsReadOnlyAccess](#)
- [AWSIOTFleetHubFederationAccess](#)
- [AWSIOTFleetwiseServiceRolePolicy](#)
- [AWSIOTFullAccess](#)
- [AWSIoTLogging](#)
- [AWSIOTOTAUpdate](#)
- [AWSIoTRoboRunnerFullAccess](#)

- [AWSIoTRoboRunnerReadOnly](#)
- [AWSIoTRoboRunnerServiceRolePolicy](#)
- [AWSIoTRuleActions](#)
- [AWSIoTSiteWiseConsoleFullAccess](#)
- [AWSIoTSiteWiseFullAccess](#)
- [AWSIoTSiteWiseMonitorPortalAccess](#)
- [AWSIoTSiteWiseMonitorServiceRolePolicy](#)
- [AWSIoTSiteWiseReadOnlyAccess](#)
- [AWSIoTThingsRegistration](#)
- [AWSIoTThingMakerServiceRolePolicy](#)
- [AWSIoTWirelessDataAccess](#)
- [AWSIoTWirelessFullAccess](#)
- [AWSIoTWirelessFullPublishAccess](#)
- [AWSIoTWirelessGatewayCertManager](#)
- [AWSIoTWirelessLogging](#)
- [AWSIoTWirelessReadOnlyAccess](#)
- [AWSIPAMServiceRolePolicy](#)
- [AWSIQContractServiceRolePolicy](#)
- [AWSIQFullAccess](#)
- [AWSIQPermissionServiceRolePolicy](#)
- [AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy](#)
- [AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy](#)
- [AWSKeyManagementServicePowerUser](#)
- [AWSLakeFormationCrossAccountManager](#)
- [AWSLakeFormationDataAdmin](#)
- [AWSLambda_FullAccess](#)
- [AWSLambda_ReadOnlyAccess](#)
- [AWSLambdaBasicExecutionRole](#)
- [AWSLambdaDynamoDBExecutionRole](#)
- [AWSLambdaENIManagementAccess](#)

- [AWSLambdaExecute](#)
- [AWSLambdaFullAccess](#)
- [AWSLambdaInvocation-DynamoDB](#)
- [AWSLambdaKinesisExecutionRole](#)
- [AWSLambdaMSKExecutionRole](#)
- [AWSLambdaReplicator](#)
- [AWSLambdaRole](#)
- [AWSLambdaSQSQueueExecutionRole](#)
- [AWSLambdaVPCAccessExecutionRole](#)
- [AWSLicenseManagerConsumptionPolicy](#)
- [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)
- [AWSLicenseManagerMasterAccountRolePolicy](#)
- [AWSLicenseManagerMemberAccountRolePolicy](#)
- [AWSLicenseManagerServiceRolePolicy](#)
- [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)
- [AWSM2ServicePolicy](#)
- [AWSManagedServices_ContactsServiceRolePolicy](#)
- [AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy](#)
- [AWSManagedServices_EventsServiceRolePolicy](#)
- [AWSManagedServicesDeploymentToolkitPolicy](#)
- [AWSMarketplaceAmiIngestion](#)
- [AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWSMarketplaceFullAccess](#)
- [AWSMarketplaceGetEntitlements](#)
- [AWSMarketplaceImageBuildFullAccess](#)
- [AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWSMarketplaceManageSubscriptions](#)
- [AWSMarketplaceMeteringFullAccess](#)
- [AWSMarketplaceMeteringRegisterUsage](#)
- [AWSMarketplaceProcurementSystemAdminFullAccess](#)

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

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

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

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

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

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

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

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

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

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

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

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

- [ViewOnlyAccess](#)
- [VMImportExportRoleForAWSConnector](#)
- [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](#)
- [WorkLink_Service_Role_Policy](#)

AccessAnalyzerServiceRolePolicy

설명: 액세스 분석기가 리소스 메타데이터를 분석하도록 허용

AccessAnalyzerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 2일, 17:13 UTC
- 편집 시간: 2024년 5월 30일 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AdministratorAccess

설명: AWS 서비스 및 리소스에 대한 전체 액세스 권한을 제공합니다.

AdministratorAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AdministratorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AdministratorAccess-Amplify

설명: Amplify 애플리케이션에 필요한 리소스에 대한 직접 액세스를 명시적으로 허용하면서 계정 관리 권한을 부여합니다.

AdministratorAccess-Amplify [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AdministratorAccess-Amplify를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 19:03 UTC
- 편집 시간: 2024년 4월 4일 20:35 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-Amplify

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

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

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



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

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

```

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

```

```
"Resource" : "*"
},
{
  "Sid" : "AmplifyStorageSDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:DeleteBucketPolicy",
    "s3:DeleteBucketWebsite",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutBucketAcl",
    "s3:PutBucketCORS",
    "s3:PutBucketNotification",
    "s3:PutBucketPolicy",
    "s3:PutBucketVersioning",
    "s3:PutBucketWebsite",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSRCalls",
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:CreateCloudFrontOriginAccessIdentity",
    "cloudfront:CreateDistribution",
    "cloudfront:CreateInvalidation",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListCloudFrontOriginAccessIdentities",
    "cloudfront:ListDistributions",
    "cloudfront:ListDistributionsByLambdaFunction",
    "cloudfront:ListDistributionsByWebACLId",
    "cloudfront:ListFieldLevelEncryptionConfigs",
```

```
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListInvalidations",
"cloudfront:ListPublicKeys",
"cloudfront:ListStreamingDistributions",
"cloudfront:UpdateDistribution",
"cloudfront:TagResource",
"cloudfront:UntagResource",
"cloudfront:ListTagsForResource",
"cloudfront:DeleteDistribution",
"iam:AttachRolePolicy",
"iam:CreateRole",
"iam:CreateServiceLinkedRole",
"iam:GetRole",
"iam:PutRolePolicy",
"iam:PassRole",
"lambda:CreateFunction",
"lambda:EnableReplication",
"lambda:DeleteFunction",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:PublishVersion",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"lambda:ListTags",
"lambda:TagResource",
"lambda:UntagResource",
"route53:ChangeResourceRecordSets",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"s3:CreateBucket",
"s3:GetAccelerateConfiguration",
"s3:GetObject",
"s3:ListBucket",
"s3:PutAccelerateConfiguration",
"s3:PutBucketPolicy",
"s3:PutObject",
"s3:PutBucketTagging",
"s3:GetBucketTagging",
"lambda:ListEventSourceMappings",
"lambda:CreateEventSourceMapping",
"iam:UpdateAssumeRolePolicy",
"iam>DeleteRolePolicy",
"sqs:CreateQueue",
"sqs>DeleteQueue",
```

```

    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "amplify:GetApp",
    "amplify:GetBranch",
    "amplify:UpdateApp",
    "amplify:UpdateBranch"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSRViewLogGroups",
  "Effect" : "Allow",
  "Action" : "logs:DescribeLogGroups",
  "Resource" : "arn:aws:logs:*:*:log-group:*"
},
{
  "Sid" : "AmplifySSRCreateLogGroup",
  "Effect" : "Allow",
  "Action" : "logs:CreateLogGroup",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
},
{
  "Sid" : "AmplifySSRPushLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AdministratorAccess-AWSElasticBeanstalk

설명: 계정 관리 권한을 부여합니다. 개발자와 관리자가 Elastic AWS Beanstalk 애플리케이션을 관리하는 데 필요한 리소스에 직접 액세스할 수 있도록 명시적으로 허용합니다.

AdministratorAccess-AWSElasticBeanstalk [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AdministratorAccess-AWSElasticBeanstalk를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 19:36 UTC
- 편집된 시간: 2023년 3월 23일, 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessDeviceSetup

설명: AlexaForBusiness 서비스에 대한 장치 설정 액세스 권한 제공

AlexaForBusinessDeviceSetup [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessDeviceSetup를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2019년 5월 20일, 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessFullAccess

설명: 리소스에 대한 전체 액세스 권한 및 관련 AlexaForBusiness 리소스에 대한 액세스 권한을 부여합니다. AWS 서비스

AlexaForBusinessFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2020년 7월 1일, 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessGatewayExecution

설명: AlexaForBusiness 서비스에 대한 게이트웨이 실행 액세스 권한 제공

AlexaForBusinessGatewayExecution [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessGatewayExecution를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2017년 11월 30일, 16:47 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

설명: Lifesize AVS 장치에 대한 액세스를 제공합니다.

AlexaForBusinessLifesizeDelegatedAccessPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessLifesizeDelegatedAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 4일, 19:46 UTC
- 편집된 시간: 2020년 6월 12일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "Action" : [
      "a4b:SearchDevices"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "a4b:filters_deviceType" : [
          "*A2IW07UEGWV4TL"
        ]
      },
      "Null" : {
        "a4b:filters_deviceType" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:AssociateDeviceWithRoom"
    ],
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL",
      "arn:aws:a4b:us-east-1:*:room/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:GetRoom",
      "a4b:GetAddressBook",
      "a4b:SearchRooms",
      "a4b:CreateContact",
      "a4b:CreateRoom",
      "a4b:UpdateContact",
      "a4b:ListConferenceProviders",
      "a4b>DeleteRoom",
      "a4b:CreateAddressBook",
      "a4b:DisassociateContactFromAddressBook",
      "a4b:CreateConferenceProvider",
      "a4b:PutConferencePreference",
      "a4b>DeleteAddressBook",
      "a4b:AssociateContactWithAddressBook",

```

```

    "a4b:DeleteContact",
    "a4b:SearchProfiles",
    "a4b:UpdateProfile",
    "a4b:GetContact"
  ],
  "Resource" : "*"
},
{
  "Action" : [
    "kms:DescribeKey"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:kms:*:*:key/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessNetworkProfileServicePolicy

설명: 이 정책을 사용하면 Alexa for Business가 네트워크 프로파일에서 예약한 자동 작업을 수행할 수 있습니다.

AlexaForBusinessNetworkProfileServicePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 3월 13일, 00:53 UTC

- 편집된 시간: 2019년 4월 5일, 21:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessPolyDelegatedAccessPolicy

설명: Poly AVS 장치에 대한 액세스를 제공합니다.

AlexaForBusinessPolyDelegatedAccessPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessPolyDelegatedAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 16일, 19:48 UTC
- 편집된 시간: 2019년 10월 16일, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AlexaForBusinessReadOnlyAccess

설명: AlexaForBusiness 서비스에 대한 읽기 전용 액세스 권한 제공

AlexaForBusinessReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2019년 11월 20일, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAPIGatewayAdministrator

설명: 를 통해 Amazon API Gateway에서 API를 생성/편집/삭제할 수 있는 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonAPIGatewayAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAPIGatewayAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:34 UTC
- 편집된 시간: 2015년 7월 9일, 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAPIGatewayInvokeFullAccess

설명: Amazon API Gateway에서 API를 호출할 수 있는 전체 액세스 권한을 제공합니다.

AmazonAPIGatewayInvokeFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAPIGatewayInvokeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:36 UTC
- 편집된 시간: 2018년 12월 18일, 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAPIGatewayPushToCloudWatchLogs

설명: API Gateway에서 사용자 계정으로 로그를 푸시할 수 있도록 허용합니다.

AmazonAPIGatewayPushToCloudWatchLogs [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAPIGatewayPushToCloudWatchLogs를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 11일, 23:41 UTC

- 편집된 시간: 2015년 11월 11일, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppFlowFullAccess

설명: Amazon에 대한 전체 액세스 AppFlow 권한과 흐름 소스 또는 대상 (S3 및 Redshift) 으로 지원되는 AWS 서비스에 대한 액세스를 제공합니다. 또한 암호화를 위해 KMS에 대한 액세스를 제공합니다.

AmazonAppFlowFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppFlowFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 2일, 23:30 UTC
- 편집된 시간: 2022년 2월 28일, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppFlowReadOnlyAccess

설명: Amazon Appflow 플로우에 대한 읽기 전용 액세스를 제공합니다.

AmazonAppFlowReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppFlowReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 2일, 23:26 UTC
- 편집된 시간: 2022년 2월 28일, 20:42 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppStreamFullAccess

설명: AppStream 를 통해 Amazon에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AmazonAppStreamFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppStreamFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 8월 28일, 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppStreamPCAAccess

설명: Amazon AppStream 2.0에서 고객 계정의 AWS Certificate Manager 사설 CA에 액세스하여 인증서 기반 인증을 수행합니다.

AmazonAppStreamPCAAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppStreamPCAAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2022년 10월 24일, 17:05 UTC
- 편집된 시간: 2022년 10월 24일, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppStreamReadOnlyAccess

설명: AppStream 를 통해 Amazon에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonAppStreamReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppStreamReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 12월 7일, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAppStreamServiceAccess

설명: Amazon AppStream 서비스 역할에 대한 기본 정책입니다.

AmazonAppStreamServiceAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppStreamServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 19일, 04:17 UTC
- 편집된 시간: 2020년 6월 26일, 16:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAthenaFullAccess

설명: Amazon Athena에 대한 전체 액세스 권한과 쿼리, 결과 작성 및 데이터 관리에 필요한 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonAthenaFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAthenaFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 16:46 UTC
- 편집 시간: 2024년 1월 3일 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAugmentedAIFullAccess

설명: 및 을 FlowDefinitions 포함하여 HumanTaskUis Amazon Augmented AI 리소스의 모든 작업을 수행할 수 있는 액세스 권한을 제공합니다. HumanLoops 퍼블릭 클라우드 워크팀을 FlowDefinitions 상 대로 창작 활동을 위한 액세스는 허용되지 않습니다.

AmazonAugmentedAIFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAugmentedAIFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:21 UTC
- 편집된 시간: 2019년 12월 3일, 16:21 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAugmentedAIHumanLoopFullAccess

설명: 모든 작업을 수행할 수 있는 액세스 권한을 제공합니다 HumanLoops.

AmazonAugmentedAIHumanLoopFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAugmentedAIHumanLoopFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:20 UTC
- 편집된 시간: 2019년 12월 3일, 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonAugmentedAIIntegratedAPIAccess

설명: 및 을 FlowDefinitions 포함하여 HumanTaskUis Amazon Augmented AI 리소스의 모든 작업을 수행할 수 있는 액세스 권한을 제공합니다. HumanLoops 또한 Amazon Augmented AI와 통합된 서비스 운영에 대한 액세스를 제공합니다.

AmazonAugmentedAIIntegratedAPIAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonAugmentedAIIntegratedAPIAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 22일, 20:47 UTC
- 편집된 시간: 2020년 4월 22일, 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonBedrockFullAccess

설명: Amazon Bedrock에 대한 전체 액세스 권한은 물론 필요한 관련 서비스에도 제한적으로 액세스할 수 있습니다.

AmazonBedrockFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBedrockFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 6일 15:47 UTC
- 편집 시간: 2023년 12월 6일, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonBedrockReadOnly

설명: Amazon Bedrock에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonBedrockReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBedrockReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 6일 15:48 UTC
- 편집 시간: 2023년 12월 6일, 15:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonBraketFullAccess

설명: AWS Management Console 및 SDK를 통해 Amazon Braket에 대한 전체 액세스 권한을 제공합니다. 또한 관련 서비스(예: S3, logs)에 대한 액세스를 제공합니다.

AmazonBraketFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBraketFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 6일, 20:12 UTC
- 편집된 시간: 2023년 4월 19일, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonBraketJobsExecutionPolicy

설명: S3, 클라우드워치, IAM AWS 서비스 및 브라켓을 포함하여 Amazon Braket Job을 실행하는 데 필요한 액세스 권한과 리소스를 부여합니다.

AmazonBraketJobsExecutionPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBraketJobsExecutionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 26일, 19:34 UTC
- 편집된 시간: 2021년 11월 28일, 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonBraketServiceRolePolicy

설명: Amazon Braket이 사용자를 대신하여 AWS 리소스를 생성하고 관리할 수 있도록 허용합니다.

AmazonBraketServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 4일, 17:12 UTC
- 편집된 시간: 2020년 8월 6일, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeFullAccess

설명: 를 통해 Amazon Chime 관리 콘솔에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonChimeFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:15 UTC
- 편집된 시간: 2020년 12월 14일, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeReadOnly

설명: 를 통해 Amazon Chime 관리 콘솔에 대한 읽기 전용 액세스 권한을 제공합니다. AWS Management Console

AmazonChimeReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:04 UTC
- 편집된 시간: 2020년 12월 14일, 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeReadOnly

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeSDK

설명: Amazon Chime SDK 작업에 대한 액세스를 제공합니다.

AmazonChimeSDK [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeSDK를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 4일, 21:53 UTC

- 편집된 시간: 2023년 1월 10일, 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

설명: Amazon Chime SDK MediaPipelines 서비스 연결 역할에 대한 관리형 정책

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 4월 4일, 22:02 UTC
- 편집 시간: 2023년 12월 8일 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeSDKMessagingServiceRolePolicy

설명: Amazon Chime SDK 메시징이 AWS 리소스에 액세스하고 메시징 기능을 활성화할 수 있도록 허용합니다.

AmazonChimeSDKMessagingServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 3일, 01:43 UTC
- 편집된 시간: 2023년 3월 3일, 01:43 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeServiceRolePolicy

설명: Amazon Chime에서 사용하거나 관리하는 AWS 리소스에 액세스할 수 있습니다.

AmazonChimeServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 9월 30일, 22:25 UTC
- 편집된 시간: 2019년 9월 30일, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

설명: Amazon Chime이 사용자를 대신하여 Amazon Transcribe 및 Amazon Transcribe Medical에 액세스할 수 있도록 허용합니다.

AmazonChimeTranscriptionServiceLinkedRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 4일, 21:47 UTC

- 편집된 시간: 2021년 8월 4일, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeUserManagement

설명: 를 통해 Amazon Chime 관리 콘솔에 대한 사용자 관리 액세스 권한을 제공합니다. AWS Management Console

AmazonChimeUserManagement [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeUserManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:17 UTC
- 편집된 시간: 2020년 2월 18일, 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

설명: Amazon Chime의 서비스 연결 역할에 대한 관리형 정책 VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 9월 30일, 22:16 UTC
- 편집된 시간: 2023년 4월 14일, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudDirectoryFullAccess

설명: Amazon Cloud Directory 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonCloudDirectoryFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudDirectoryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 25일, 00:41 UTC
- 편집된 시간: 2017년 2월 25일, 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudDirectoryReadOnlyAccess

설명: Amazon Cloud Directory 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonCloudDirectoryReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudDirectoryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 28일, 23:42 UTC
- 편집된 시간: 2017년 2월 28일, 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchEvidentlyFullAccess

설명: Amazon에 대한 전체 액세스 권한만 제공합니다 CloudWatch . 또한 관련 Amazon S3, Amazon SNS CloudWatch, Amazon 및 기타 관련 서비스에 대한 액세스를 제공합니다.

AmazonCloudWatchEvidentlyFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchEvidentlyFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:10 UTC
- 편집된 시간: 2021년 11월 29일, 15:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

설명: Amazon에 대한 읽기 전용 액세스 권한을 CloudWatch 분명히 제공합니다.

AmazonCloudWatchEvidentlyReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchEvidentlyReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:08 UTC
- 편집된 시간: 2021년 11월 29일, 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

설명: CloudWatch Evidently Service가 고객을 대신하여 관련 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonCloudWatchEvidentlyServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 13일, 17:25 UTC
- 편집된 시간: 2022년 9월 13일, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchRUMFullAccess

설명: Amazon CloudWatch RUM 서비스에 대한 전체 액세스 권한을 부여합니다.

AmazonCloudWatchRUMFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchRUMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:46 UTC
- 편집된 시간: 2021년 11월 29일, 15:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```



```
"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:*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchRUMReadOnlyAccess

설명: Amazon CloudWatch RUM 서비스에 대한 읽기 전용 권한을 부여합니다.

AmazonCloudWatchRUMReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchRUMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:43 UTC
- 편집된 시간: 2022년 10월 28일, 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCloudWatchRUMServiceRolePolicy

설명: Amazon CloudWatch RUM 서비스에 모니터링 데이터를 다른 관련 AWS 서비스에 게시할 수 있는 권한을 부여합니다.

AmazonCloudWatchRUMServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 23:17 UTC
- 편집된 시간: 2023년 2월 22일, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeCatalystFullAccess

설명: Amazon에 대한 전체 액세스 권한을 제공합니다. CodeCatalyst

AmazonCodeCatalystFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeCatalystFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 20일, 16:50 UTC
- 편집된 시간: 2023년 4월 20일, 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeCatalystReadOnlyAccess

설명: Amazon에 대한 읽기 전용 액세스를 제공합니다. CodeCatalyst

AmazonCodeCatalystReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeCatalystReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 20일, 16:49 UTC
- 편집된 시간: 2023년 4월 20일, 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```

    "codecatalyst:Get*",
    "codecatalyst:List*"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeCatalystSupportAccess

설명: Amazon이 CodeCatalyst 셀러를 대신하여 AWS Support 사례를 생성, 업데이트 및 해결할 수 있도록 허용합니다.

AmazonCodeCatalystSupportAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeCatalystSupportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 12:34 UTC
- 편집된 시간: 2023년 4월 20일, 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruProfilerAgentAccess

설명: Amazon CodeGuru 프로파일러 에이전트가 필요로 하는 액세스 권한을 제공합니다.

AmazonCodeGuruProfilerAgentAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruProfilerAgentAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 5일, 22:11 UTC
- 편집된 시간: 2022년 5월 5일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruProfilerFullAccess

설명: Amazon CodeGuru 프로파일러에 대한 전체 액세스 권한을 제공합니다.

AmazonCodeGuruProfilerFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruProfilerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 10:13 UTC
- 편집된 시간: 2020년 7월 15일, 03:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruProfilerReadOnlyAccess

설명: Amazon CodeGuru 프로파일러에 대한 읽기 전용 액세스를 제공합니다.

AmazonCodeGuruProfilerReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruProfilerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 10:30 UTC
- 편집된 시간: 2020년 6월 27일, 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruReviewerFullAccess

설명: Amazon CodeGuru Reviewer에 대한 전체 액세스 권한과 필수 종속성에 대한 범위 지정 액세스 권한을 부여합니다.

AmazonCodeGuruReviewerFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruReviewerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 08:33 UTC
- 편집된 시간: 2020년 8월 29일, 04:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruReviewerReadOnlyAccess

설명: Amazon CodeGuru 리뷰어에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonCodeGuruReviewerReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruReviewerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 08:48 UTC

- 편집된 시간: 2020년 8월 29일, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruReviewerServiceRolePolicy

설명: Amazon CodeGuru Reviewer가 사용자를 대신하여 리소스에 액세스하려면 서비스 연결 역할이 필요합니다.

AmazonCodeGuruReviewerServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 3일, 05:31 UTC
- 편집된 시간: 2020년 11월 27일, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruSecurityFullAccess

설명: Amazon CodeGuru 보안에 대한 전체 액세스 권한을 제공합니다.

AmazonCodeGuruSecurityFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruSecurityFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 9일, 21:03 UTC
- 편집된 시간: 2023년 5월 9일, 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCodeGuruSecurityScanAccess

설명: Amazon CodeGuru 보안 스캔을 사용하는 데 필요한 액세스 권한을 제공합니다.

AmazonCodeGuruSecurityScanAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruSecurityScanAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 9일, 20:54 UTC
- 편집된 시간: 2023년 5월 9일, 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoDeveloperAuthenticatedIdentities

설명: 인증 백엔드에서 개발자 인증 자격 증명을 지원하기 위해 Amazon Cognito API에 대한 액세스를 제공합니다.

AmazonCognitoDeveloperAuthenticatedIdentities [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoDeveloperAuthenticatedIdentities를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:22 UTC
- 편집된 시간: 2015년 3월 24일, 17:22 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonCognitoDeveloperAuthenticatedIdentities

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoIdpEmailServiceRolePolicy

설명: Amazon Cognito 사용자 풀 서비스가 이메일 전송에 SES ID를 사용할 수 있도록 허용합니다.

AmazonCognitoIdpEmailServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 3월 21일, 21:32 UTC
- 편집된 시간: 2019년 3월 21일, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoIdpServiceRolePolicy

설명: Amazon Cognito 사용자 풀에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다.

AmazonCognitoIdpServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 26일, 22:30 UTC
- 편집된 시간: 2020년 6월 26일, 22:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoPowerUser

설명: 기존 Amazon Cognito 리소스에 대한 관리 액세스를 제공합니다. 새 Cognito 리소스를 생성하려면 AWS 계정 관리자 권한이 필요합니다.

AmazonCognitoPowerUser [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:14 UTC
- 편집된 시간: 2021년 6월 1일, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoReadOnly

설명: Amazon Cognito 리소스에 대한 읽기 전용 액세스를 제공합니다.

AmazonCognitoReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:06 UTC
- 편집된 시간: 2019년 8월 1일, 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

설명: 이 정책은 Cognito 자격 증명 풀의 인증되지 않은 자격 증명에 허용되는 권한 세트를 정의합니다. 이 정책은 독립형 권한 정책으로 사용하기 위한 것이 아닙니다. 이는 자격 증명 풀의 역할에 연결된 지나치게 허용적인 정책을 막기 위한 가드레일로 사용됩니다. Cognito Identity Service는 자격 증명을 생성할 때 자동으로 범위 축소 정책으로 포함하므로 이 정책을 어떤 역할에도 연결하지 마십시오. 향상된 흐름을 통해 다른 AWS 리소스에 일시적으로 액세스할 수 있는 권한은 이제 서비스에서 제공하는 인증되지 않은 사용자의 ID와 관련된 역할과 Cognito가 소유한 이 관리형 정책에 부여된 권한의 교차점에 의해 정의됩니다.

AmazonCognitoUnAuthedIdentitiesSessionPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoUnAuthedIdentitiesSessionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 19일, 23:04 UTC
- 편집된 시간: 2023년 7월 19일, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonCognitoUnauthenticatedIdentities

설명: 이 정책은 Cognito 자격 증명 풀의 인증되지 않은 자격 증명에 허용되는 권한 세트를 정의합니다. Cognito Identity Service는 자격 증명을 생성할 때 자동으로 범위 축소 정책으로 포함하므로 이를

unauth 역할에 연결할 필요가 없습니다. 향상된 흐름을 통해 다른 AWS 리소스에 일시적으로 액세스할 수 있는 권한은 이제 서비스에서 제공하는 인증되지 않은 사용자의 ID와 관련된 역할과 Cognito가 소유한 이 관리형 정책에 부여된 권한의 교차점에 의해 정의됩니다.

AmazonCognitoUnauthenticatedIdentities [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoUnauthenticatedIdentities를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 1일, 22:36 UTC
- 편집된 시간: 2023년 2월 1일, 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnect_FullAccess

설명: 이 정책의 목적은 Connect 리소스를 사용하는 데 필요한 권한을 AWS Connect 사용자에게 부여하는 것입니다. 이 정책은 Connect 콘솔 및 퍼블릭 API를 통해 AWS Connect 리소스에 대한 전체 액세스를 제공합니다.

AmazonConnect_FullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonConnect_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 19:54 UTC
- 편집된 시간: 2023년 3월 7일, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

설명: Amazon Connect 캠페인 서비스 연결 역할에 대한 정책

AmazonConnectCampaignsServiceLinkedRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 23일, 20:54 UTC
- 편집된 시간: 2023년 11월 8일, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnectReadOnlyAccess

설명: 사용자의 Amazon Connect 인스턴스를 볼 수 있는 권한을 AWS 계정부여합니다.

AmazonConnectReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonConnectReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 17일, 21:00 UTC
- 편집된 시간: 2019년 11월 6일, 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnectServiceLinkedRolePolicy

설명: Amazon Connect가 사용자를 대신하여 AWS 리소스를 생성하고 관리할 수 있도록 허용합니다.

AmazonConnectServiceLinkedRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 9월 7일, 00:21 UTC
- 편집 시간: 2024년 5월 24일 01:42 UTC

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

정책 버전

정책 버전: v16(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnectSynchronizationServiceRolePolicy

설명: Amazon Connect가 사용자 대신 여러 지역의 AWS 리소스를 동기화할 수 있도록 허용합니다.

AmazonConnectSynchronizationServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 10월 27일, 22:38 UTC

- 편집된 시간: 2023년 10월 27일, 22:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonConnectVoiceIDFullAccess

설명: Amazon Connect 음성 ID에 대한 전체 액세스 권한을 제공합니다.

AmazonConnectVoiceIDFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonConnectVoiceIDFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 26일, 19:04 UTC
- 편집된 시간: 2021년 9월 26일, 19:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneDomainExecutionRolePolicy

설명: DataZone Amazon의 DomainExecutionRole 서비스 역할에 대한 기본 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다.

AmazonDataZoneDomainExecutionRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneDomainExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2023년 9월 27일, 21:55 UTC
- 편집 시간: 2024년 4월 1일 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

설명: Amazon은 데이터 분석 작업을 수행할 환경에 대한 IAM 역할을 DataZone 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의합니다.

AmazonDataZoneEnvironmentRolePermissionsBoundary [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneEnvironmentRolePermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 11일, 23:38 UTC
- 편집 시간: 2023년 11월 17일 23:29 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteBlueprint",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeleteConnection",
"glue>DeleteCrawler",
"glue>DeleteJob",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
"glue>DeleteTable",
"glue>DeleteTableVersion",
"glue>DeleteWorkflow",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:PutWorkflowRunProperties",
"glue:ResetJobBookmark",
"glue:ResumeWorkflowRun",
"glue:SearchTables",
"glue:StartBlueprintRun",
"glue:StartCrawler",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:StopCrawler",
"glue:StopCrawlerSchedule",
"glue:StopWorkflowRun",
"glue:UpdateBlueprint",
"glue:UpdateColumnStatisticsForPartition",
```

```

    "glue:UpdateColumnStatisticsForTable",
    "glue:UpdateConnection",
    "glue:UpdateCrawler",
    "glue:UpdateCrawlerSchedule",
    "glue:UpdateDatabase",
    "glue:UpdateJob",
    "glue:UpdatePartition",
    "glue:UpdateTable",
    "glue:UpdateWorkflow"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "PassRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/datazone*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "glue.amazonaws.com"
    }
  }
},
{
  "Sid" : "SameAccountKmsOperations",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "KmsOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:Verify",
    "kms:Sign"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AnalyticsOperations",
  "Effect" : "Allow",
  "Action" : [
    "datzone:*",
    "sqlworkbench:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QueryOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena>DeleteNamedQuery",
    "athena>DeleteNotebook",
```

```
"athena:DeletePreparedStatement",
"athena:ExportNotebook",
"athena:GetDatabase",
"athena:GetDataCatalog",
"athena:GetNamedQuery",
"athena:GetPreparedStatement",
"athena:GetQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryRuntimeStatistics",
"athena:GetTableMetadata",
"athena:GetWorkGroup",
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatements",
"athena:ListQueryExecutions",
"athena:ListTableMetadata",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"athena:StartCalculationExecution",
"athena:StartQueryExecution",
"athena:StartSession",
"athena:StopCalculationExecution",
"athena:StopQueryExecution",
"athena:TerminateSession",
"athena:UpdateNamedQuery",
"athena:UpdateNotebook",
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:Describe*",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition",
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetWorkflows",
"glue:BatchUpdatePartition",
"glue:CreateBlueprint",
"glue:CreateConnection",
```

```
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
"glue>DeleteTable",
"glue>DeleteTableVersion",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:SearchTables",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateDatabase",
"glue:UpdatePartition",
"glue:UpdateTable",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListGroups",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUsers",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:DescribeMetricFilters",
"logs:DescribeQueries",
"logs:DescribeQueryDefinitions",
"logs:DescribeMetricFilters",
"logs:StartQuery",
```

```

    "logs:StopQuery",
    "logs:GetLogEvents",
    "logs:GetLogGroupFields",
    "logs:GetQueryResults",
    "logs:GetLogRecord",
    "logs:PutLogEvents",
    "logs:CreateLogStream",
    "logs:FilterLogEvents",
    "lakeformation:GetDataAccess",
    "lakeformation:GetDataLakeSettings",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListPermissions",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:DescribeStatement",
    "redshift:CreateClusterUser",
    "redshift:DescribeClusters",
    "redshift:DescribeDataShares",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:JoinGroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "secretsmanager:ListSecrets",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QueryOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryResultsStream"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {

```

```

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

```



```
  },
  {
    "Sid" : "DataZoneS3BucketLocation",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListDataZoneS3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "s3:prefix" : [
          "*/datazone/*",
          "datazone/*"
        ]
      }
    }
  },
  {
    "Sid" : "NotDeniedOperations",
    "Effect" : "Deny",
    "NotAction" : [
      "datazone:*",
      "sqlworkbench:*",
      "athena:BatchGetNamedQuery",
      "athena:BatchGetPreparedStatement",
      "athena:BatchGetQueryExecution",
      "athena:CreateNamedQuery",
      "athena:CreateNotebook",
      "athena:CreatePreparedStatement",
      "athena:CreatePresignedNotebookUrl",
      "athena>DeleteNamedQuery",
      "athena>DeleteNotebook",
      "athena>DeletePreparedStatement",
      "athena:ExportNotebook",
```

```
"athena:GetDatabase",
"athena:GetDataCatalog",
"athena:GetNamedQuery",
"athena:GetPreparedStatement",
"athena:GetQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryResultsStream",
"athena:GetQueryRuntimeStatistics",
"athena:GetTableMetadata",
"athena:GetWorkGroup",
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatements",
"athena:ListQueryExecutions",
"athena:ListTableMetadata",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"athena:StartCalculationExecution",
"athena:StartQueryExecution",
"athena:StartSession",
"athena:StopCalculationExecution",
"athena:StopQueryExecution",
"athena:TerminateSession",
"athena:UpdateNamedQuery",
"athena:UpdateNotebook",
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"ec2:CreateNetworkInterface",
"ec2:CreateTags",
"ec2>DeleteNetworkInterface",
"ec2>DeleteTags",
"ec2:Describe*",
"glue:*DataQuality*",
"glue:BatchCreatePartition",
"glue:BatchDeleteConnection",
"glue:BatchDeletePartition",
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetWorkflows",
```

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

```
"glue:StopCrawlerSchedule",
"glue:StopWorkflowRun",
"glue:UpdateBlueprint",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateConnection",
"glue:UpdateCrawler",
"glue:UpdateCrawlerSchedule",
"glue:UpdateDatabase",
"glue:UpdateJob",
"glue:UpdatePartition",
"glue:UpdateTable",
"glue:UpdateWorkflow",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:List*",
"iam:PassRole",
"kms:DescribeKey",
"kms:Decrypt",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:ListKeys",
"kms:Verify",
"kms:Sign",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:DescribeMetricFilters",
"logs:DescribeQueries",
"logs:DescribeQueryDefinitions",
"logs:StartQuery",
"logs:StopQuery",
"logs:GetLogEvents",
"logs:GetLogGroupFields",
"logs:GetQueryResults",
"logs:GetLogRecord",
"logs:PutLogEvents",
"logs:CreateLogStream",
"logs:FilterLogEvents",
"lakeformation:GetDataAccess",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetResourceLFTags",
"lakeformation:ListPermissions",
"redshift-data:ListTables",
"redshift-data:DescribeTable",
```

```

    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:DescribeStatement",
    "redshift:CreateClusterUser",
    "redshift:DescribeClusters",
    "redshift:DescribeDataShares",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:JoinGroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:CreateSecret",
    "secretsmanager:ListSecrets",
    "secretsmanager:TagResource",
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneFullAccess

설명: DataZone Amazon에 대한 전체 액세스 권한은 AWS Management Console 물론 필요한 관련 서비스에 대한 제한된 액세스를 제공합니다.

AmazonDataZoneFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 22일, 20:06 UTC
- 편집 시간: 2024년 4월 23일 21:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-datzone*"
},
{
    "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_*"
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneFullUserAccess

설명: DataZone Amazon에 대한 전체 액세스를 제공하지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다.

AmazonDataZoneFullUserAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneFullUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 22일, 21:06 UTC
- 편집 시간: 2024년 4월 1일 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneGlueManageAccessRolePolicy

설명: 이 정책은 Amazon이 데이터에 대한 게시 및 액세스 권한을 DataZone 허용할 수 있는 권한을 부여합니다.

AmazonDataZoneGlueManageAccessRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneGlueManageAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 9월 22일, 20:21 UTC
- 편집 시간: 2024년 6월 3일 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZonePortalFullAccessPolicy

설명: Amazon DataZone API에 대한 전체 액세스 권한을 제공합니다.

AmazonDataZonePortalFullAccessPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZonePortalFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 26일, 18:24 UTC
- 편집된 시간: 2023년 3월 26일, 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZonePreviewConsoleFullAccess

설명: 를 DataZone 통해 Amazon의 프리뷰 릴리스에 대한 전체 액세스 권한을 제공합니다 AWS Management Console. 또한 관련 서비스에 대한 선택적 액세스를 제공합니다.

AmazonDataZonePreviewConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZonePreviewConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 28일, 15:16 UTC
- 편집된 시간: 2023년 7월 13일, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

설명: Amazon은 데이터 분석 프로젝트를 배포하는 데 사용하는 IAM 역할을 DataZone 생성합니다. DataZone 권한의 경계를 정의하기 위해 이러한 역할을 생성할 때 이 정책을 사용합니다.

AmazonDataZoneProjectDeploymentPermissionsBoundary [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneProjectDeploymentPermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 21일, 02:54 UTC
- 편집된 시간: 2023년 4월 4일, 02:48 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneProjectDeploymentPermissionsBoundary

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneProjectRolePermissionsBoundary

설명: Amazon은 프로젝트에서 데이터 분석 작업을 수행할 IAM 역할을 DataZone 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한 범위를 정의합니다.

AmazonDataZoneProjectRolePermissionsBoundary [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneProjectRolePermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 21일, 02:51 UTC
- 편집된 시간: 2023년 3월 21일, 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

설명: DataZone Amazon은 데이터를 카탈로그, 검색, 관리, 공유 및 분석할 수 있는 데이터 관리 서비스입니다. DataZoneAmazon을 사용하면 계정 및 지원 지역 전반에서 데이터를 공유하고 액세스할 수 있습니다. Amazon은 Amazon Redshift, Amazon Athena, AWS Glue 및 Lake Formation을 포함하되 이에 국한되지 않는 AWS 서비스 전반에서 사용자 경험을 DataZone 단순화합니다. AWS

AmazonDataZoneRedshiftGlueProvisioningPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneRedshiftGlueProvisioningPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 22일, 20:19 UTC
- 편집 시간: 2024년 3월 12일 16:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    }
  }
}

```



```

    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

설명: 이 정책은 Amazon에 Amazon Redshift 데이터를 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 카탈로그에 있는 Amazon Redshift 또는 Amazon Redshift 서버리스에 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 아마존에 부여합니다.

AmazonDataZoneRedshiftManageAccessRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneRedshiftManageAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 9월 22일, 20:15 UTC
- 편집 시간: 2023년 11월 16일 22:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

설명: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 정책은 Amazon이 프로비저닝한 SageMaker 환경에서 생성된 실행 역할에 허용되는 권한 목록입니다. DataZone

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 23일 23:01 UTC
- 편집 시간: 2024년 5월 8일 02:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

설명: 이 AmazonDataZoneSageMakerManageAccessRolePolicy 정책은 사용자에게 SageMaker 환경의 다양한 리소스에 대한 액세스 권한을 부여하는 데 필요한 권한을 DataZone Amazon에 부여합니다.

AmazonDataZoneSageMakerManageAccessRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneSageMakerManageAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 23일 23:34 UTC
- 편집 시간: 2024년 4월 23일 23:34 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

설명: 이 AmazonDataZoneSageMakerProvisioningRolePolicy 정책은 DataZone Amazon과 상호 운용하는 데 필요한 권한을 SageMaker Amazon에 부여합니다.

AmazonDataZoneSageMakerProvisioningRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneSageMakerProvisioningRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 23일 23:32 UTC
- 편집 시간: 2024년 4월 23일 23:32 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerProvisioningRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDetectiveFullAccess

설명: Amazon Detective 서비스에 대한 전체 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonDetectiveFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDetectiveFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 30일, 17:57 UTC
- 편집된 시간: 2023년 5월 17일, 19:39 UTC

- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDetectiveInvestigatorAccess

설명: 조사자에게 Amazon Detective 서비스에 대한 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다. 이 정책은 조사 목적으로 Detective를 사용할 수 있는 권한을 부여하고 Guardduty에 대한 제한된 쓰기 액세스를 부여합니다.

AmazonDetectiveInvestigatorAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDetectiveInvestigatorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 17일, 15:24 UTC
- 편집 시간: 2023년 11월 27일 03:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDetectiveMemberAccess

설명: Amazon Detective 서비스에 대한 구성원 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonDetectiveMemberAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDetectiveMemberAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 17일, 15:16 UTC
- 편집된 시간: 2023년 1월 17일, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatatypes",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```


}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDetectiveOrganizationsAccess

설명: Amazon Detective의 위임된 관리자 및 콘솔 UI 종속성에 대한 범위 지정 액세스를 관리할 수 있는 Organizations 액세스 권한을 제공합니다. 또한 Detective에 대한 서비스 연결 역할을 생성할 수 있는 권한을 부여합니다.

AmazonDetectiveOrganizationsAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDetectiveOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 2일, 15:20 UTC
- 편집된 시간: 2023년 3월 2일, 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ],
  "Statement" : [
    {
      "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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDetectiveServiceLinkedRolePolicy

설명: Amazon Detective가 사용자를 대신하여 서비스 호출을 할 수 있도록 허용합니다.

AmazonDetectiveServiceLinkedRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 18일, 19:47 UTC
- 편집된 시간: 2021년 11월 18일, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDevOpsGuruConsoleFullAccess

설명: 이 정책은 DevOps Guru 콘솔에 대한 전체 액세스 권한을 부여합니다.

AmazonDevOpsGuruConsoleFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 12월 17일, 18:43 UTC
- 편집된 시간: 2022년 8월 25일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDevOpsGuruFullAccess

설명: Amazon DevOps Guru에 대한 전체 액세스 권한을 제공합니다.

AmazonDevOpsGuruFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:38 UTC
- 편집된 시간: 2022년 8월 25일, 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDevOpsGuruOrganizationsAccess

설명: 조직 내에서 Amazon DevOps Guru를 활성화하고 관리할 수 있는 액세스 권한을 제공합니다.

AmazonDevOpsGuruOrganizationsAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 15일, 23:50 UTC
- 편집된 시간: 2021년 11월 15일, 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
```


- 편집된 시간: 2022년 8월 25일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  }  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDevOpsGuruServiceRolePolicy

설명: Amazon이 리소스에 DevOpsGuru 액세스하려면 서비스 연결 역할이 필요합니다.

AmazonDevOpsGuruServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 1일, 10:24 UTC
- 편집된 시간: 2023년 1월 10일, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
}

```

```
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDMSCloudWatchLogsRole

설명: 고객 계정의 cloudwatch 로그에 DMS 복제 로그를 업로드할 수 있는 액세스 권한을 제공합니다.

AmazonDMSCloudWatchLogsRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDMSCloudWatchLogsRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 7일, 23:44 UTC
- 편집된 시간: 2023년 5월 23일, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDMSRedshiftS3Role

설명: DMS용 Redshift 엔드포인트의 S3 설정을 관리하기 위한 액세스를 제공합니다.

AmazonDMSRedshiftS3Role [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDMSRedshiftS3Role를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 4월 20일, 17:05 UTC
- 편집된 시간: 2019년 7월 8일, 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDMSVPCManagementRole

설명: AWS 관리형 고객 구성의 VPC 설정을 관리할 수 있는 액세스 권한을 제공합니다.

AmazonDMSVPCManagementRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDMSVPCManagementRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 18일, 16:33 UTC
- 편집된 시간: 2016년 5월 23일, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDB-ElasticServiceRolePolicy

설명: Amazon DocumentDB-Elastic이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonDocDB-ElasticServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 30일, 14:17 UTC
- 편집된 시간: 2022년 11월 30일, 14:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDBConsoleFullAccess

설명: 를 사용하여 MongoDB와 호환되는 Amazon DocumentDB를 관리할 수 있는 전체 액세스 권한을 제공합니다. AWS Management Console참고로 이 정책은 또한 계정 내의 모든 SNS 주제에 대해 게시할 수 있는 전체 액세스, Amazon EC2 인스턴스 및 VPC 구성을 생성 및 편집할 수 있는 권한, Amazon

KMS에서 키를 보고 나열할 수 있는 권한, Amazon RDS 및 Amazon Neptune에 대한 전체 액세스도 부여합니다.

AmazonDocDBConsoleFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:37 UTC
- 편집된 시간: 2022년 11월 30일, 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic>DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic>DeleteClusterSnapshot",

```

```
"docdb-elastic:ListClusterSnapshots",
"docdb-elastic:RestoreClusterFromSnapshot",
"docdb-elastic:TagResource",
"docdb-elastic:UntagResource",
"docdb-elastic:ListTagsForResource",
"rds:AddRoleToDBCluster",
"rds:AddSourceIdentifierToSubscription",
"rds:AddTagsToResource",
"rds:ApplyPendingMaintenanceAction",
"rds:CopyDBClusterParameterGroup",
"rds:CopyDBClusterSnapshot",
"rds:CopyDBParameterGroup",
"rds>CreateDBCluster",
"rds>CreateDBClusterParameterGroup",
"rds>CreateDBClusterSnapshot",
"rds>CreateDBInstance",
"rds>CreateDBParameterGroup",
"rds>CreateDBSubnetGroup",
"rds>CreateEventSubscription",
"rds>CreateGlobalCluster",
"rds>DeleteDBCluster",
"rds>DeleteDBClusterParameterGroup",
"rds>DeleteDBClusterSnapshot",
"rds>DeleteDBInstance",
"rds>DeleteDBParameterGroup",
"rds>DeleteDBSubnetGroup",
"rds>DeleteEventSubscription",
"rds>DeleteGlobalCluster",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
```

```

    "rds:DescribeEventCategories",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeEvents",
    "rds:DescribeGlobalClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DescribeValidDBInstanceModifications",
    "rds:DownloadDBLogFilePortion",
    "rds:FailoverDBCluster",
    "rds:ListTagsForResource",
    "rds:ModifyDBCluster",
    "rds:ModifyDBClusterParameterGroup",
    "rds:ModifyDBClusterSnapshotAttribute",
    "rds:ModifyDBInstance",
    "rds:ModifyDBParameterGroup",
    "rds:ModifyDBSubnetGroup",
    "rds:ModifyEventSubscription",
    "rds:ModifyGlobalCluster",
    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveFromGlobalCluster",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsForResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:AllocateAddress",
    "ec2:AssignIpv6Addresses",
    "ec2:AssignPrivateIpAddresses",

```

```
"ec2:AssociateAddress",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AssociateVpcCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:CreateCustomerGateway",
"ec2:CreateDefaultSubnet",
"ec2:CreateDefaultVpc",
"ec2:CreateInternetGateway",
"ec2:CreateNatGateway",
"ec2:CreateNetworkInterface",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCustomerGateways",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVpcAttribute",
"ec2:ModifyVpcEndpoint",
"kms:DescribeKey",
"kms:ListAliases",
"kms:ListKeyPolicies",
"kms:ListKeys",
"kms:ListRetirableGrants",
"logs:DescribeLogStreams",
"logs:GetLogEvents",
```

```

        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "rds.amazonaws.com"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
    }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDBElasticFullAccess

설명: Amazon DocumentDB 엘라스틱 클러스터에 대한 전체 액세스 권한과 EC2, KMS, IAM을 비롯한 해당 클러스터의 종속 항목에 대한 기타 필수 권한을 제공합니다. SecretsManager CloudWatch

AmazonDocDBElasticFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBElasticFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 5일, 13:51 UTC
- 편집된 시간: 2023년 6월 21일, 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDBElasticReadOnlyAccess

설명: Amazon DocDB-Elastic 및 지표에 대한 읽기 전용 액세스를 제공합니다. CloudWatch

AmazonDocDBElasticReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBElasticReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 8일, 14:37 UTC
- 편집된 시간: 2023년 6월 21일, 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDBFullAccess

설명: MongoDB와 호환되는 Amazon DocumentDB에 대한 전체 액세스 권한을 제공합니다. 참고로 이 정책은 계정 내 모든 SNS 주제에 대한 게시에 대한 전체 액세스와 Amazon RDS 및 Amazon Neptune에 대한 전체 액세스도 부여합니다.

AmazonDocDBFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:21 UTC
- 편집된 시간: 2019년 1월 9일, 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDocDBReadOnlyAccess

설명: MongoDB와 호환되는 Amazon DocumentDB에 대한 읽기 전용 액세스를 제공합니다. 참고로 이 정책은 Amazon RDS 및 Amazon Neptune 리소스에 대한 액세스 권한도 부여합니다.

AmazonDocDBReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:30 UTC
- 편집된 시간: 2019년 1월 9일, 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDRSVPCManagement

설명: Amazon 관리형 고객 구성의 VPC 설정을 관리할 수 있는 액세스 권한을 제공합니다.

AmazonDRSVPCManagement [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDRSVPCManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 9월 2일, 00:09 UTC
- 편집된 시간: 2015년 9월 2일, 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDynamoDBFullAccess

설명: 를 통해 Amazon DynamoDB에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonDynamoDBFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2021년 1월 29일, 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDynamoDBFullAccesswithDataPipeline

설명: 이 정책은 지원 중단될 예정입니다. 지침은 설명서를 참조하세요. <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html> 를 통한 Data Pipeline을 AWS 사용한 내보내기/가져오기를 포함하여 Amazon DynamoDB에 대한 전체 액세스를 제공합니다. AWS Management Console

AmazonDynamoDBFullAccesswithDataPipeline [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBFullAccesswithDataPipeline를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 11월 12일, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonDynamoDBReadOnlyAccess

설명: 를 통해 Amazon DynamoDB에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonDynamoDBReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 3월 20일 15:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEBSCSIDriverPolicy

설명: CSI 드라이버 서비스 계정이 사용자 대신 EC2와 같은 관련 서비스를 호출할 수 있도록 허용하는 IAM 정책입니다.

AmazonEBSCSIDriverPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEBSCSIDriverPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 4일, 17:24 UTC
- 편집된 시간: 2022년 11월 18일, 14:42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerRegistryFullAccess

설명: Amazon ECR 리소스에 대한 관리 액세스를 제공합니다.

AmazonEC2ContainerRegistryFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:06 UTC
- 편집된 시간: 2020년 12월 5일, 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerRegistryPowerUser

설명: Amazon EC2 컨테이너 레지스트리 리포지토리에 대한 전체 액세스를 제공하지만 리포지토리 삭제 또는 정책 변경은 허용하지 않습니다.

AmazonEC2ContainerRegistryPowerUser [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerRegistryPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:05 UTC
- 편집된 시간: 2019년 12월 10일, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerRegistryReadOnly

설명: Amazon EC2 컨테이너 레지스트리 리포지토리에 대한 읽기 전용 액세스를 제공합니다.

AmazonEC2ContainerRegistryReadOnly [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerRegistryReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:04 UTC
- 편집된 시간: 2019년 12월 10일, 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerServiceAutoscaleRole

설명: Amazon EC2 Container Service의 작업 자동 크기 조정을 활성화하는 정책

AmazonEC2ContainerServiceAutoscaleRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerServiceAutoscaleRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 5월 12일, 23:25 UTC
- 편집된 시간: 2018년 2월 5일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerServiceEventsRole

설명: EC2 컨테이너 서비스용 CloudWatch 이벤트를 활성화하는 정책

AmazonEC2ContainerServiceEventsRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerServiceEventsRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 5월 30일, 16:51 UTC
- 편집된 시간: 2023년 3월 6일, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerServiceforEC2Role

설명: Amazon EC2 컨테이너 서비스를 위한 Amazon EC2 역할에 대한 기본 정책입니다.

AmazonEC2ContainerServiceforEC2Role [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerServiceforEC2Role를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 3월 19일, 18:45 UTC
- 편집된 시간: 2023년 3월 6일, 22:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ContainerServiceRole

설명: Amazon ECS 서비스 역할에 대한 기본 정책입니다.

AmazonEC2ContainerServiceRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 16:14 UTC
- 편집된 시간: 2016년 8월 11일, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2FullAccess

설명: 를 통해 Amazon EC2에 대한 전체 액세스를 제공합니다. AWS Management Console

AmazonEC2FullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2018년 11월 27일, 02:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2ReadOnlyAccess

설명: 를 통해 Amazon EC2에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonEC2ReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 2월 14일 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2RoleforAWSCodeDeploy

설명: 수정 버전을 다운로드할 수 있도록 S3 버킷에 대한 EC2 액세스를 제공합니다. 이 역할은 EC2 인스턴스의 CodeDeploy 에이전트에 필요합니다.

AmazonEC2RoleforAWSCodeDeploy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforAWSCodeDeploy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 19일, 18:10 UTC

- 편집된 시간: 2017년 3월 20일, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2RoleforAWSCodeDeployLimited

설명: 수정 버전을 다운로드할 수 있도록 S3 버킷에 대한 EC2의 제한된 액세스를 제공합니다. 이 역할은 EC2 인스턴스의 CodeDeploy 에이전트에 필요합니다.

AmazonEC2RoleforAWSCodeDeployLimited [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforAWSCodeDeployLimited를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 24일, 17:55 UTC
- 편집된 시간: 2022년 1월 20일, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2RoleforDataPipelineRole

설명: 데이터 파이프라인용 Amazon EC2 역할 서비스 역할에 대한 기본 정책입니다.

AmazonEC2RoleforDataPipelineRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforDataPipelineRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집된 시간: 2016년 2월 22일, 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2RoleforSSM

설명: 이 정책은 곧 지원 중단될 예정입니다. AmazonSSM ManagedInstanceCore 정책을 사용하여 EC2 인스턴스에서 AWS Systems Manager 서비스 핵심 기능을 활성화하십시오. 자세한 내용은 <https://docs.aws.amazon.com/systems-manager/latest/userguide/.html>을 참조하십시오. setup-instance-profile

AmazonEC2RoleforSSM [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforSSM를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 29일, 17:48 UTC
- 편집된 시간: 2019년 1월 24일, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2RolePolicyForLaunchWizard

설명: EC2용 Amazon LaunchWizard 서비스 역할에 대한 관리형 정책

AmazonEC2RolePolicyForLaunchWizard [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RolePolicyForLaunchWizard를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 08:05 UTC
- 편집된 시간: 2022년 5월 16일, 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2SpotFleetAutoscaleRole

설명: Amazon EC2 스팟 플릿의 자동 크기 조정을 활성화하는 정책

AmazonEC2SpotFleetAutoscaleRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2SpotFleetAutoscaleRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 8월 19일, 18:27 UTC
- 편집된 시간: 2019년 2월 18일, 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEC2SpotFleetTaggingRole

설명: EC2 스팟 플릿이 사용자를 대신하여 스팟 인스턴스를 요청, 종료 및 태깅할 수 있도록 허용합니다.

AmazonEC2SpotFleetTaggingRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2SpotFleetTaggingRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 6월 29일, 18:19 UTC
- 편집된 시간: 2020년 4월 23일, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonECS_FullAccess

설명: Amazon ECS 리소스에 대한 관리 액세스를 제공하고 VPC, Auto Scaling 그룹 및 스택을 비롯한 다른 AWS 서비스 리소스에 대한 액세스를 통해 ECS 기능을 활성화합니다. CloudFormation

AmazonECS_FullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonECS_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 7일, 21:36 UTC
- 편집된 시간: 2023년 1월 4일, 16:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

정책 버전

정책 버전: v20(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    ]
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

설명: 사용자를 대신하여 ECS Service Connect TLS 기능을 관리하는 AWS 서비스 데 필요한 사설 인증 기관, AWS Secrets Manager 및 기타 기능에 대한 관리 액세스를 제공합니다.

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 작성 시간: 2024년 1월 19일 20:08 UTC
- 편집 시간: 2024년 1월 19일 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        }
      }
    }
  ]
}
```

```

    "StringEquals" : {
      "aws:RequestTag/AmazonECSManaged" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  },
  {
    "Sid" : "RotateTLSCertificateSecret",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DescribeSecret",
      "secretsmanager:UpdateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue",
      "secretsmanager>DeleteSecret",
      "secretsmanager:RotateSecret",
      "secretsmanager:UpdateSecretVersionStage"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthority",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:GetCertificate",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:DescribeCertificateAuthority"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSManaged" : "true"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
    "Effect" : "Allow",

```

```

    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSTemplateArn" : "true",
        "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonECSInfrastructureRolePolicyForVolumes

설명: 사용자 대신 ECS 워크로드와 관련된 볼륨을 관리하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공합니다.

AmazonECSInfrastructureRolePolicyForVolumes [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonECSInfrastructureRolePolicyForVolumes를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 작성 시간: 2024년 1월 10일 22:56 UTC
- 편집 시간: 2024년 1월 10일 22:56 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "DescribeVolumesForLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVolumes",
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ManageEBSVolumeLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
},
{
  "Sid" : "ManageVolumeAttachmentsForEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*"
},
{
  "Sid" : "DeleteEBSManagedVolume",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteVolume",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "ArnLike" : {
      "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
    }
  }
},
```

```

    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonECSServiceRolePolicy

설명: Amazon ECS에서 클러스터를 관리할 수 있도록 하는 정책입니다.

AmazonECSServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 14일, 01:18 UTC
- 편집 시간: 2023년 12월 4일 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonECSTaskExecutionRolePolicy

설명: Amazon ECS 작업을 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공합니다.

AmazonECSTaskExecutionRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonECSTaskExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 16일, 18:48 UTC
- 편집된 시간: 2017년 11월 16일, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
```

```
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEFSCSIDriverPolicy

설명: EFS 리소스에 대한 관리 액세스 및 EC2에 대한 읽기 액세스를 제공합니다.

AmazonEFSCSIDriverPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEFSCSIDriverPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 7월 25일, 20:10 UTC
- 편집된 시간: 2023년 7월 25일, 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKS_CNI_Policy

설명: 이 정책은 Amazon VPC CNI 플러그인 (amazon-vpc-cni-k8s) 에 EKS 작업자 노드의 IP 주소 구성을 수정하는 데 필요한 권한을 제공합니다. 이 권한 세트를 통해 CNI는 사용자를 대신하여 Elastic Network Interfaces를 나열, 설명 및 수정할 수 있습니다. AWS VPC CNI 플러그인에 대한 자세한 내용은 다음에서 확인할 수 있습니다. <https://github.com/aws/8s-amazon-vpc-cni-k>

AmazonEKS_CNI_Policy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKS_CNI_Policy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:07 UTC
- 편집 시간: 2024년 3월 4일 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSClusterPolicy

설명: 이 정책은 사용자를 대신하여 리소스를 관리하는 데 필요한 권한을 Kubernetes에 제공합니다. 쿠버네티스에는 인스턴스, 보안 그룹, 엘라스틱 네트워크 인터페이스를 포함하나 이에 국한되지 않는 EC2 리소스에 식별 정보를 배치할 수 있는 Ec2: CreateTags 권한이 필요합니다.

AmazonEKSClusterPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSClusterPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 5월 27일, 21:06 UTC
- 편집된 시간: 2023년 2월 7일, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSCoordinatorServiceRolePolicy

설명: 이 정책은 Amazon EKS에서 EKS 커넥터의 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonEKSCoordinatorServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 4일, 20:31 UTC
- 편집된 시간: 2021년 9월 4일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSFargatePodExecutionRolePolicy

설명: Fargate에서 Amazon EKS 포드를 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공합니다. AWS

AmazonEKSFargatePodExecutionRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSFargatePodExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 22일, 04:34 UTC
- 편집된 시간: 2019년 11월 22일, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "Effect" : "Allow",
    "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSFargateServiceRolePolicy

설명: 이 정책은 fargate 작업을 실행하는 데 필요한 권한을 Amazon EKS에 부여합니다.

AmazonEKSFargateServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 22일, 04:36 UTC
- 편집된 시간: 2019년 11월 22일, 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSLocalOutpostClusterPolicy

설명: 이 정책은 사용자 계정에서 실행되는 EKS 로컬 클러스터의 컨트롤 플레인 인스턴스에 사용자 대신 리소스를 관리할 수 있는 권한을 제공합니다.

AmazonEKSLocalOutpostClusterPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSLocalOutpostClusterPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 24일, 21:56 UTC
- 편집된 시간: 2022년 10월 17일, 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSLocalOutpostServiceRolePolicy

설명: Amazon EKS Local에서 사용자를 대신하여 AWS 서비스에 전화를 걸 수 있습니다.

AmazonEKSLocalOutpostServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 8월 23일, 21:53 UTC
- 편집된 시간: 2022년 10월 24일, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSServicePolicy

설명: 이 정책은 Kubernetes용 Amazon Elastic Container Service에서 EKS 클러스터를 운영하는 데 필요한 리소스를 생성하고 관리할 수 있도록 허용합니다.

AmazonEKSServicePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSServicePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:08 UTC
- 편집된 시간: 2020년 5월 27일, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSServiceRolePolicy

설명: Amazon EKS가 사용자를 대신하여 AWS 서비스를 호출하려면 서비스 연결 역할이 필요합니다.

AmazonEKSServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 2월 21일, 20:10 UTC
- 편집된 시간: 2020년 5월 27일, 19:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSVPCResourceController

설명: VPC 리소스 컨트롤러에서 작업자 노드의 ENI 및 IP를 관리하는 데 사용하는 정책입니다.

AmazonEKSVPCResourceController [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSVPCResourceController를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 12일, 00:55 UTC
- 편집된 시간: 2020년 8월 12일, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEKSWorkerNodePolicy

설명: 이 정책은 Amazon EKS 작업자 노드가 Amazon EKS 클러스터에 연결할 수 있도록 허용합니다.

AmazonEKSWorkerNodePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSWorkerNodePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:09 UTC
- 편집 시간: 2023년 11월 27일 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElastiCacheFullAccess

설명: ElastiCache 를 통해 Amazon에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AmazonElastiCacheFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElastiCacheFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 11월 28일 03:49 UTC

- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElastiCacheReadOnlyAccess

설명: ElastiCache 를 통해 Amazon에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonElastiCacheReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElastiCacheReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticCacheReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticContainerRegistryPublicFullAccess

설명: Amazon ECR 퍼블릭 리소스에 대한 관리 액세스를 제공합니다.

AmazonElasticContainerRegistryPublicFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticContainerRegistryPublicFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 17:25 UTC
- 편집된 시간: 2020년 12월 1일, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticContainerRegistryPublicPowerUser

설명: Amazon ECR Public 리포지토리에 대한 전체 액세스를 제공하지만 리포지토리 삭제 또는 정책 변경은 허용하지 않습니다.

AmazonElasticContainerRegistryPublicPowerUser [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticContainerRegistryPublicPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:16 UTC
- 편집된 시간: 2020년 12월 1일, 16:16 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicPowerUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticContainerRegistryPublicReadOnly

설명: Amazon ECR 퍼블릭 리포지토리에 대한 읽기 전용 액세스를 제공합니다.

AmazonElasticContainerRegistryPublicReadOnly [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticContainerRegistryPublicReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 17:27 UTC
- 편집된 시간: 2020년 12월 1일, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemClientFullAccess

설명: Amazon EFS 파일 시스템에 대한 루트 클라이언트 액세스를 제공합니다.

AmazonElasticFileSystemClientFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemClientFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 13일, 16:27 UTC
- 편집된 시간: 2020년 1월 13일, 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemClientReadOnlyAccess

설명: Amazon EFS 파일 시스템에 대한 읽기 전용 클라이언트 액세스를 제공합니다.

AmazonElasticFileSystemClientReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemClientReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2020년 1월 13일, 16:24 UTC
- 편집된 시간: 2020년 1월 13일, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemClientReadWriteAccess

설명: Amazon EFS 파일 시스템에 대한 읽기 및 쓰기 클라이언트 액세스를 제공합니다.

AmazonElasticFileSystemClientReadWriteAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemClientReadWriteAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 13일, 16:21 UTC
- 편집된 시간: 2020년 1월 13일, 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemFullAccess

설명: 를 통해 Amazon EFS에 대한 전체 액세스를 제공합니다 AWS Management Console.

AmazonElasticFileSystemFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 27일, 16:22 UTC
- 편집 시간: 2023년 11월 28일 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemReadOnlyAccess

설명: 를 통해 Amazon EFS에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonElasticFileSystemReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 27일, 16:25 UTC
- 편집된 시간: 2022년 1월 10일, 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemServiceRolePolicy

설명: Amazon Elastic File System에서 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 합니다.

AmazonElasticFileSystemServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 5일, 16:52 UTC
- 편집된 시간: 2022년 1월 10일, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticFileSystemsUtils

설명: 고객이 AWS Systems Manager를 사용하여 EC2 인스턴스의 Amazon EFS 유틸리티 (amazon-efs-utils) 패키지를 자동으로 관리하고 EFS 파일 시스템 탑재 성공/실패 알림을 받는 CloudWatchLog 데 사용할 수 있습니다.

AmazonElasticFileSystemsUtils [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemsUtils를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 29일, 15:16 UTC
- 편집된 시간: 2020년 9월 29일, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceEditorsRole

설명: Amazon Elastic MapReduce Editors 서비스 역할에 대한 기본 정책입니다.

AmazonElasticMapReduceEditorsRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceEditorsRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 16일, 21:55 UTC
- 편집된 시간: 2023년 2월 9일, 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceforAutoScalingRole

설명: Auto MapReduce Scaling을 위한 Amazon Elastic. Auto Scaling이 EMR 클러스터에서 인스턴스를 추가 및 제거할 수 있도록 허용하는 역할입니다.

AmazonElasticMapReduceforAutoScalingRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceforAutoScalingRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 18일, 01:09 UTC
- 편집된 시간: 2016년 11월 18일, 01:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceforEC2Role

설명: EC2용 Amazon Elastic 서비스 역할에 MapReduce 대한 기본 정책입니다.

AmazonElasticMapReduceforEC2Role [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceforEC2Role를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2017년 8월 11일, 23:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceFullAccess

설명: 이 정책은 지원 중단될 예정입니다. 지침은 <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies/> .html 설명서를 참조하십시오. Amazon Elastic MapReduce 및 EC2 및 S3와 같이 필요한 기본 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonElasticMapReduceFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 10월 11일, 15:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReducePlacementGroupPolicy

설명: EMR이 EC2 배치 그룹을 생성, 설명 및 삭제할 수 있도록 허용하는 정책입니다.

AmazonElasticMapReducePlacementGroupPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReducePlacementGroupPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 29일, 00:37 UTC
- 편집된 시간: 2020년 9월 29일, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceReadOnlyAccess

설명: 를 MapReduce 통해 Amazon Elastic에 대한 읽기 전용 액세스 권한을 제공합니다 AWS Management Console.

AmazonElasticMapReduceReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 7월 29일, 23:14 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticMapReduceRole

설명: 이 정책은 지원 중단될 예정입니다. 지침에 대한 지침은 <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies/.html> 설명서를 참조하십시오. Amazon Elastic MapReduce 서비스 역할에 대한 기본 정책입니다.

AmazonElasticMapReduceRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2020년 6월 24일, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticsearchServiceRolePolicy

설명: Amazon Elasticsearch Service가 사용자를 대신하여 EC2 네트워킹 API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용하십시오.

AmazonElasticsearchServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 7월 7일, 00:15 UTC
- 편집된 시간: 2023년 10월 23일, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticTranscoder_FullAccess

설명: 사용자에게 Elastic Transcoder에 대한 전체 액세스 권한과 Elastic Transcoder의 전체 기능에 필요한 관련 서비스에 대한 액세스 권한을 부여합니다.

AmazonElasticTranscoder_FullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoder_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 27일, 18:59 UTC

- 편집된 시간: 2019년 6월 10일, 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticTranscoder_JobsSubmitter

설명: 사용자에게 프리셋을 변경하고, 작업을 제출하고, Elastic Transcoder 설정을 볼 수 있는 권한을 부여합니다. 또한 이 정책은 Elastic Transcode 콘솔을 사용하는 데 필요한 일부 다른 서비스(S3, IAM, SNS등)에 대한 읽기 전용 액세스 권한도 일부 부여합니다.

AmazonElasticTranscoder_JobsSubmitter [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoder_JobsSubmitter를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 7일, 21:12 UTC
- 편집된 시간: 2019년 6월 10일, 22:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticTranscoder_ReadOnlyAccess

설명: 사용자에게 Elastic Transcoder에 대한 읽기 전용 액세스 권한과 관련 서비스에 대한 목록 액세스 권한을 부여합니다.

AmazonElasticTranscoder_ReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoder_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 7일, 21:09 UTC
- 편집된 시간: 2019년 6월 10일, 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonElasticTranscoderRole

설명: Amazon Elastic Transcoder 서비스 역할에 대한 기본 정책입니다.

AmazonElasticTranscoderRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoderRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2019년 6월 13일, 22:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRCleanupPolicy

설명: EMR 서비스 역할이 해당 기능을 상실한 경우 EMR에서 AWS EC2 리소스를 종료 및 삭제하는데 필요한 작업을 허용합니다.

AmazonEMRCleanupPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 26일, 23:54 UTC
- 편집된 시간: 2020년 9월 29일, 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRContainersServiceRolePolicy

설명: Amazon EMR을 실행하는 데 필요한 다른 AWS 서비스 리소스에 액세스할 수 있습니다.

AmazonEMRContainersServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 9일, 00:38 UTC
- 편집된 시간: 2023년 3월 10일, 22:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRFullAccessPolicy_v2

설명: Amazon EMR에 대한 전체 액세스 권한을 제공합니다.

AmazonEMRFullAccessPolicy_v2 [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRFullAccessPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 12일, 01:50 UTC
- 편집된 시간: 2023년 7월 28일, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRReadOnlyAccessPolicy_v2

설명: Amazon EMR 및 관련 CloudWatch 지표에 대한 읽기 전용 액세스를 제공합니다.

AmazonEMRReadOnlyAccessPolicy_v2 [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRReadOnlyAccessPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 12일, 01:39 UTC
- 편집된 시간: 2023년 8월 2일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRServerlessServiceRolePolicy

설명: Amazon EMRserverless를 실행하는 데 필요한 다른 AWS 서비스 리소스에 액세스할 수 있습니다.

AmazonEMRServerlessServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 5월 20일, 23:15 UTC
- 편집 시간: 2024년 1월 25일 18:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEMRServicePolicy_v2

설명: 이 정책은 Amazon EMR 서비스 역할에 사용되며 계정 내 다른 IAM 사용자 또는 역할에는 사용해서는 안 됩니다. 이 정책은 EMR 클러스터 운영에 필요한 EMR 및 관련 서비스와 연관된 리소스를 생성하고 관리할 수 있는 권한을 부여합니다.

AmazonEMRServicePolicy_v2 [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRServicePolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 3월 12일, 01:11 UTC
- 편집 시간: 2024년 5월 2일 18:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonESCognitoAccess

설명: Amazon Cognito 구성 서비스에 대한 제한된 액세스를 제공합니다.

AmazonESCognitoAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonESCognitoAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 28일, 22:29 UTC

- 편집된 시간: 2021년 12월 20일, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonESFullAccess

설명: Amazon ES 구성 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonESFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonESFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 1일, 19:14 UTC
- 편집된 시간: 2015년 10월 1일, 19:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonESReadOnlyAccess

설명: Amazon ES 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonESReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonESReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 10월 1일, 19:18 UTC
- 편집된 시간: 2018년 10월 3일, 03:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

설명: 사용자를 대신하여 시크릿 매니저 리소스에 액세스할 수 있습니다. EventBridge

AmazonEventBridgeApiDestinationsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 2월 11일, 20:52 UTC
- 편집된 시간: 2021년 2월 11일, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeFullAccess

설명: Amazon에 대한 전체 액세스 권한을 제공합니다 EventBridge.

AmazonEventBridgeFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 11일, 14:08 UTC
- 편집된 시간: 2022년 12월 1일, 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgePipesFullAccess

설명: Amazon EventBridge Pipes에 대한 전체 액세스 권한을 제공합니다.

AmazonEventBridgePipesFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgePipesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 12월 1일, 17:03 UTC
- 편집된 시간: 2022년 12월 1일, 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgePipesOperatorAccess

설명: Amazon EventBridge Pipes에 대한 읽기 전용 및 운영자 (파이프 실행을 중지하고 시작할 수 있는 기능) 액세스를 제공합니다.

AmazonEventBridgePipesOperatorAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgePipesOperatorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 12월 1일, 17:04 UTC
- 편집된 시간: 2022년 12월 1일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgePipesReadOnlyAccess

설명: Amazon EventBridge Pipes에 대한 읽기 전용 액세스를 제공합니다.

AmazonEventBridgePipesReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgePipesReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 12월 1일, 17:04 UTC
- 편집된 시간: 2022년 12월 1일, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeReadOnlyAccess

설명: Amazon에 대한 읽기 전용 액세스를 제공합니다 EventBridge.

AmazonEventBridgeReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 11일, 13:59 UTC
- 편집된 시간: 2022년 12월 1일, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeSchedulerFullAccess

설명: AmazonEventBridgeSchedulerFullAccess 관리형 정책은 일정 및 일정 그룹에 대한 모든 EventBridge 스케줄러 작업을 사용할 수 있는 권한을 부여합니다.

AmazonEventBridgeSchedulerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchedulerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 18:37 UTC
- 편집된 시간: 2022년 11월 10일, 18:37 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeSchedulerReadOnlyAccess

설명: AmazonEventBridgeSchedulerReadOnlyAccess 관리형 정책은 일정 및 일정 그룹에 대한 세부 정보를 볼 수 있는 읽기 전용 권한을 부여합니다.

AmazonEventBridgeSchedulerReadOnlyAccess [AWS 관리형 정책입니다](#).

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchedulerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 18:50 UTC
- 편집된 시간: 2022년 11월 10일, 18:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ]
    }
  ]
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeSchemasFullAccess

설명: Amazon EventBridge 스키마에 대한 전체 액세스 권한을 제공합니다.

AmazonEventBridgeSchemasFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchemasFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 28일, 23:12 UTC
- 편집된 시간: 2019년 11월 28일, 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeSchemasReadOnlyAccess

설명: Amazon EventBridge 스키마에 대한 읽기 전용 액세스를 제공합니다.

AmazonEventBridgeSchemasReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchemasReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 28일, 23:05 UTC
- 편집된 시간: 2020년 5월 1일, 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonEventBridgeSchemasServiceRolePolicy

설명: Amazon EventBridge 스키마에서 생성한 관리형 규칙에 권한을 부여합니다.

AmazonEventBridgeSchemasServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 27일, 01:10 UTC

- 편집된 시간: 2019년 11월 27일, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFISServiceRolePolicy

설명: AWS FIS가 실험을 위한 모니터링 및 리소스 선택을 관리할 수 있도록 하는 정책.

AmazonFISServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 21일, 21:18 UTC
- 편집된 시간: 2022년 10월 25일, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonForecastFullAccess

설명: Amazon Forecast의 모든 작업에 액세스할 수 있습니다.

AmazonForecastFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonForecastFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 01:52 UTC
- 편집된 시간: 2019년 1월 18일, 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFraudDetectorFullAccessPolicy

설명: Amazon Fraud Detector의 모든 작업에 대한 액세스 권한을 제공합니다.

AmazonFraudDetectorFullAccessPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFraudDetectorFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 22:46 UTC
- 편집된 시간: 2019년 12월 3일, 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFreeRTOSFullAccess

설명: Amazon Freertos에 대한 전체 액세스 정책

AmazonFreeRTOSFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFreeRTOSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 15:32 UTC
- 편집된 시간: 2017년 11월 29일, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFreeRTOSOTAUpdate

설명: 사용자가 Amazon FreeRTOS OTA 업데이트에 액세스할 수 있도록 허용합니다.

AmazonFreeRTOSOTAUpdate [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFreeRTOSOTAUpdate를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 8월 27일, 22:43 UTC
- 편집된 시간: 2020년 12월 18일, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFSxConsoleFullAccess

설명: Amazon FSx에 대한 전체 액세스 권한과 를 통해 AWS 관련 서비스에 대한 액세스를 제공합니다. AWS Management Console

AmazonFSxConsoleFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:36 UTC
- 편집 시간: 2024년 1월 10일 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
            ]
        }
    }
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFSxConsoleReadOnlyAccess

설명: Amazon FSx에 대한 읽기 전용 액세스 권한과 를 통한 AWS 관련 서비스 액세스를 제공합니다.
AWS Management Console

AmazonFSxConsoleReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 11월 28일, 16:35 UTC
- 편집 시간: 2024년 1월 10일 20:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFSxFullAccess

설명: Amazon FSx에 대한 전체 액세스 권한과 관련 서비스에 대한 액세스를 제공합니다. AWS

AmazonFSxFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:34 UTC
- 편집 시간: 2024년 1월 10일 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Sid" : "ViewAWSDDirectories",
"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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFSxReadOnlyAccess

설명: Amazon FSx에 대한 읽기 전용 액세스를 제공합니다.

AmazonFSxReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:33 UTC
- 편집된 시간: 2018년 11월 28일, 16:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonFSxServiceRolePolicy

설명: Amazon FSx가 사용자를 대신하여 리소스를 AWS 관리할 수 있도록 허용합니다.

AmazonFSxServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 28일, 10:38 UTC
- 편집 시간: 2024년 1월 10일 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGlacierFullAccess

설명: 를 통해 Amazon Glacier에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonGlacierFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGlacierFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGlacierReadOnlyAccess

설명: 를 통해 Amazon Glacier에 대한 읽기 전용 액세스 권한을 제공합니다. AWS Management Console

AmazonGlacierReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGlacierReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 5월 5일, 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGrafanaAthenaAccess

설명: 이 정책은 Amazon Grafana의 Amazon Athena 플러그인에서 s3에 결과를 쿼리하고 쓸 수 있도록 하는 데 필요한 종속성과 Amazon Athena에 대한 액세스 권한을 부여합니다.

AmazonGrafanaAthenaAccess관리형 [AWS 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonGrafanaAthenaAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 22일, 17:11 UTC
- 편집된 시간: 2021년 11월 22일, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGrafanaCloudWatchAccess

설명: 이 정책은 Amazon CloudWatch Managed Grafana 내에서 데이터 CloudWatch 소스로 사용하는 데 필요한 종속성과 Amazon에 대한 액세스 권한을 부여합니다.

AmazonGrafanaCloudWatchAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonGrafanaCloudWatchAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 3월 24일, 22:41 UTC
- 편집된 시간: 2023년 3월 24일, 22:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGrafanaRedshiftAccess

설명: 이 정책은 Amazon Redshift에 대한 범위 지정 액세스 권한과 Amazon Grafana의 Amazon Redshift 플러그인을 사용하는 데 필요한 종속성을 부여합니다.

AmazonGrafanaRedshiftAccess관리형 [AWS 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonGrafanaRedshiftAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 26일, 23:15 UTC
- 편집된 시간: 2021년 11월 26일, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGrafanaServiceLinkedRolePolicy

설명: Amazon Grafana에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

AmazonGrafanaServiceLinkedRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 8일, 23:10 UTC
- 편집된 시간: 2022년 11월 8일, 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGuardDutyFullAccess

설명: Amazon을 사용할 수 있는 전체 액세스 권한을 제공합니다 GuardDuty.

AmazonGuardDutyFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGuardDutyFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 28일, 22:31 UTC
- 편집 시간: 2024년 6월 10일 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

설명: GuardDuty 멀웨어 보호는 이름이 지정된 서비스 연결 역할 (SLR) 을 사용합니다.

AWSServiceRoleForAmazonGuardDutyMalwareProtection 이 서비스 연결 역할을 통해 GuardDuty 멀웨어 보호 기능은 에이전트 없이 검사를 수행하여 멀웨어를 탐지할 수 있습니다. GuardDuty 이를

통해 계정에서 스냅샷을 만들고 이 스냅샷을 서비스 계정과 공유하여 멀웨어를 검사할 수 있습니다. GuardDuty 이러한 공유 스냅샷을 평가하여 검색된 EC2 인스턴스 메타데이터를 멀웨어 보호 결과에 포함합니다. GuardDuty AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할은 멀웨어 보호.guarddduty.amazonaws.com 서비스가 역할을 맡을 것으로 신뢰합니다.

AmazonGuardDutyMalwareProtectionServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 19일, 19:06 UTC
- 편집 시간: 2024년 1월 25일 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGuardDutyReadOnlyAccess

설명: Amazon GuardDuty 리소스에 대한 읽기 전용 액세스를 제공합니다.

AmazonGuardDutyReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGuardDutyReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 28일, 22:29 UTC
- 편집 시간: 2023년 11월 16일 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonGuardDutyServiceRolePolicy

설명: Amazon Guard Duty에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다.

AmazonGuardDutyServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 28일, 20:12 UTC
- 편집 시간: 2024년 3월 27일 00:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHealthLakeFullAccess

설명: Amazon HealthLake 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonHealthLakeFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonHealthLakeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 2월 17일, 01:07 UTC
- 편집된 시간: 2021년 2월 17일, 01:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHealthLakeReadOnlyAccess

설명: Amazon HealthLake 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonHealthLakeReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonHealthLakeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 02:43 UTC
- 편집된 시간: 2021년 2월 17일, 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeFullAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode에 대한 전체 액세스 권한을 제공합니다.

AmazonHoneycodeFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 6월 24일, 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeReadOnlyAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode에 대한 읽기 전용 액세스를 제공합니다.

AmazonHoneycodeReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeServiceRolePolicy

설명: Amazon Honeycode가 리소스에 액세스하려면 서비스 연결 역할이 필요합니다.

AmazonHoneycodeServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 18일, 18:03 UTC
- 편집된 시간: 2020년 11월 18일, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeTeamAssociationFullAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode 팀 어소시에이션에 대한 전체 액세스 권한을 제공합니다.

AmazonHoneycodeTeamAssociationFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeTeamAssociationFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 6월 24일, 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode 팀 어소시에이션에 대한 읽기 전용 액세스를 제공합니다.

AmazonHoneycodeTeamAssociationReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeTeamAssociationReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2020년 6월 24일, 20:27 UTC
- 편집된 시간: 2020년 6월 24일, 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeWorkbookFullAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode 워크북에 대한 전체 액세스 권한을 제공합니다.

AmazonHoneycodeWorkbookFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeWorkbookFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonHoneycodeWorkbookReadOnlyAccess

설명: AWS Management Console 및 SDK를 통해 Honeycode 워크북에 대한 읽기 전용 액세스를 제공합니다.

AmazonHoneycodeWorkbookReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeWorkbookReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspector2AgentlessServiceRolePolicy

설명: Amazon Inspector에 에이전트 없는 보안 평가를 수행하는 데 AWS 서비스 필요한 액세스 권한을 부여합니다.

AmazonInspector2AgentlessServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2023년 11월 20일 15:18 UTC
- 편집 시간: 2023년 11월 20일, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}

```

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspector2FullAccess

설명: Amazon Inspector에 대한 전체 액세스 권한과 조직과 같은 기타 관련 서비스에 대한 액세스를 제공합니다.

AmazonInspector2FullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspector2FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 19:10 UTC
- 편집 시간: 2024년 4월 25일 13:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspector2ManagedCisPolicy

설명: 이 정책은 CIS 스캔을 위해 고객이 자신의 역할에 연결해야 하는 관리형 정책입니다.

AmazonInspector2ManagedCisPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspector2ManagedCisPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 1월 24일 16:31 UTC
- 편집 시간: 2024년 1월 24일 16:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspector2ReadOnlyAccess

설명: Amazon inspector2 서비스 및 관련 지원 서비스에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonInspector2ReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspector2ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 1월 21일, 14:45 UTC
- 편집된 시간: 2023년 9월 22일, 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspector2ServiceRolePolicy

설명: Amazon Inspector에 보안 평가를 수행하는 데 AWS 서비스 필요한 액세스 권한을 부여합니다.

AmazonInspector2ServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 16일, 20:27 UTC
- 편집 시간: 2024년 1월 22일 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspectorFullAccess

설명: Amazon Inspector에 대한 전체 액세스 권한을 제공합니다.

AmazonInspectorFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspectorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 17:08 UTC
- 편집된 시간: 2017년 12월 21일, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspectorReadOnlyAccess

설명: Amazon Inspector에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonInspectorReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspectorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 17:08 UTC
- 편집된 시간: 2019년 10월 1일, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonInspectorServiceRolePolicy

설명: Amazon Inspector에 보안 평가를 수행하는 데 AWS 서비스 필요한 액세스 권한을 부여합니다.

AmazonInspectorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 21일, 15:48 UTC
- 편집된 시간: 2020년 9월 11일, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKendraFullAccess

설명: 를 통해 Amazon Kendra에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonKendraFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKendraFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:15 UTC
- 편집된 시간: 2019년 12월 3일, 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKendraReadOnlyAccess

설명: 를 통해 Amazon Kendra에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonKendraReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKendraReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:13 UTC
- 편집된 시간: 2021년 5월 27일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKeyspacesFullAccess

설명: Amazon Keyspace에 대한 전체 액세스 권한 제공

AmazonKeyspacesFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKeyspacesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 23일, 17:06 UTC
- 편집된 시간: 2023년 10월 3일, 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKeyspacesReadOnlyAccess

설명: Amazon Keyspace에 대한 읽기 전용 액세스 권한 제공

AmazonKeyspacesReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKeyspacesReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 23일, 17:07 UTC
- 편집된 시간: 2022년 7월 7일, 14:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKeyspacesReadOnlyAccess_v2

설명: Amazon Keyspaces 및 관련 AWS 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonKeyspacesReadOnlyAccess_v2 [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonKeyspacesReadOnlyAccess_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 12일, 17:01 UTC
- 편집된 시간: 2023년 9월 12일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisAnalyticsFullAccess

설명: 를 통해 AWS Management Console Amazon Kinesis Analytics에 대한 전체 액세스 권한을 제공합니다.

AmazonKinesisAnalyticsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisAnalyticsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 9월 21일, 19:01 UTC
- 편집된 시간: 2016년 9월 21일, 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisAnalyticsReadOnly

설명: 를 통해 Amazon Kinesis Analytics에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonKinesisAnalyticsReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisAnalyticsReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 9월 21일, 18:16 UTC
- 편집된 시간: 2016년 9월 21일, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisFirehoseFullAccess

설명: 모든 Amazon Kinesis Firehose 전송 스트림에 대한 전체 액세스 권한을 제공합니다.

AmazonKinesisFirehoseFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisFirehoseFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 18:45 UTC
- 편집된 시간: 2015년 10월 7일, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

{
  "Action" : [
    "firehose:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisFirehoseReadOnlyAccess

설명: 모든 Amazon Kinesis Firehose 전송 스트림에 대한 읽기 전용 액세스를 제공합니다.

AmazonKinesisFirehoseReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisFirehoseReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 18:43 UTC
- 편집된 시간: 2015년 10월 7일, 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisFullAccess

설명: 를 통해 모든 스트림에 대한 전체 액세스를 제공합니다 AWS Management Console.

AmazonKinesisFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisReadOnlyAccess

설명: 를 통해 모든 스트림에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonKinesisReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  ]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisVideoStreamsFullAccess

설명: 를 통해 AWS Management Console Amazon Kinesis Video Streams에 대한 전체 액세스 권한을 제공합니다.

AmazonKinesisVideoStreamsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisVideoStreamsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 1일, 23:27 UTC
- 편집된 시간: 2017년 12월 1일, 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonKinesisVideoStreamsReadOnlyAccess

설명: 를 통해 AWS AWS Management Console Kinesis Video Streams에 대한 읽기 전용 액세스를 제공합니다.

AmazonKinesisVideoStreamsReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisVideoStreamsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 1일, 23:14 UTC
- 편집된 시간: 2017년 12월 1일, 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLaunchWizard_Fullaccess

설명: AWS Launch Wizard 및 기타 필수 서비스에 대한 전체 액세스 권한

AmazonLaunchWizard_Fullaccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLaunchWizard_Fullaccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 6일, 17:47 UTC
- 편집된 시간: 2023년 2월 22일, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:DeleteOpsMetadadata",
    "Resource" : "arn:aws:ssm:*:*:opsmetadadata/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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLaunchWizardFullAccessV2

설명: AWS Launch Wizard 및 기타 필수 서비스에 대한 전체 액세스 권한

AmazonLaunchWizardFullAccessV2 [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLaunchWizardFullAccessV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 1일, 17:14 UTC
- 편집된 시간: 2023년 9월 1일, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexChannelsAccess

설명: 이 정책을 통해 고객은 채널에서 Lex runtime을 호출할 수 있습니다.

AmazonLexChannelsAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 13일, 20:12 UTC
- 편집된 시간: 2021년 1월 13일, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Statement" : [
  {
    "Action" : [
      "lex:ListBots"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexFullAccess

설명: 를 통해 Amazon Lex에 대한 전체 액세스 권한을 제공합니다 AWS Management Console. 또한 Lex 서비스 연결 역할을 생성하고 Lex에 제한된 Lambda 함수 세트를 호출할 수 있는 권한을 부여할 수 있는 액세스를 제공합니다.

AmazonLexFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLexFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:20 UTC
- 편집 시간: 2024년 4월 16일 20:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexReadOnly

설명: Amazon Lex에 대한 읽기 전용 액세스를 제공합니다.

AmazonLexReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLexReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:13 UTC
- 편집 시간: 2024년 5월 13일 16:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexReadOnly

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexReplicationPolicy

설명: Amazon Lex가 사용자를 대신하여 여러 지역에 Lex 리소스를 복제할 수 있도록 허용합니다.

AmazonLexReplicationPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 1월 31일 23:29 UTC
- 편집 시간: 2024년 3월 8일 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexRunBotsOnly

설명: Amazon Lex 대화형 API에 대한 액세스를 제공합니다.

AmazonLexRunBotsOnly [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonLexRunBotsOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:06 UTC
- 편집된 시간: 2021년 8월 18일, 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLexV2BotPolicy

설명: 사용자를 대신하여 다른 AWS 서비스를 호출할 수 있는 Lex V2 봇 액세스를 제공합니다.

AmazonLexV2BotPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 13일, 20:10 UTC
- 편집된 시간: 2021년 1월 13일, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutEquipmentFullAccess

설명: Amazon Lookout for Equipment 운영에 대한 전체 액세스 권한을 제공합니다.

AmazonLookoutEquipmentFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutEquipmentFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 8일, 15:52 UTC
- 편집된 시간: 2021년 11월 24일, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutEquipmentReadOnlyAccess

설명: Amazon Lookout 장비에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonLookoutEquipmentReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutEquipmentReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 5일, 16:47 UTC
- 편집된 시간: 2022년 11월 10일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutMetricsFullAccess

설명: Amazon Lookout for Metrics의 모든 작업에 대한 액세스 권한을 제공합니다.

AmazonLookoutMetricsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutMetricsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 7일, 00:43 UTC
- 편집된 시간: 2021년 5월 7일, 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutMetricsReadOnlyAccess

설명: Amazon Lookout for Metrics의 모든 읽기 전용 작업에 대한 액세스 권한을 제공합니다.

AmazonLookoutMetricsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutMetricsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 7일, 00:43 UTC
- 편집된 시간: 2022년 1월 4일, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutVisionConsoleFullAccess

설명: Amazon Lookout for Vision에 대한 전체 액세스 권한과 필수 서비스 및 콘솔 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonLookoutVisionConsoleFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:37 UTC
- 편집된 시간: 2021년 5월 11일, 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutVisionConsoleReadOnlyAccess

설명: Amazon Lookout for Vision에 대한 읽기 전용 액세스 권한과 필수 서비스 및 콘솔 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonLookoutVisionConsoleReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:32 UTC
- 편집된 시간: 2021년 12월 9일, 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutVisionFullAccess

설명: Amazon Lookout for Vision에 대한 전체 액세스 권한과 필수 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonLookoutVisionFullAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:24 UTC
- 편집된 시간: 2021년 5월 11일, 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonLookoutVisionReadOnlyAccess

설명: Amazon Lookout for Vision에 대한 읽기 전용 액세스 권한과 필수 종속성에 대한 범위 지정 액세스를 제공합니다.

AmazonLookoutVisionReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:11 UTC
- 편집된 시간: 2021년 12월 9일, 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningBatchPredictionsAccess

설명: 사용자에게 Amazon Machine Learning 배치 예측을 요청할 권한을 부여합니다.

AmazonMachineLearningBatchPredictionsAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningBatchPredictionsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:12 UTC
- 편집된 시간: 2015년 4월 9일, 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ]
    }
  ]
}
```



```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningCreateOnlyAccess

설명: 예측이 불가능한 Amazon Machine Learning 리소스에 대한 생성 액세스를 제공합니다.

AmazonMachineLearningCreateOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningCreateOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:18 UTC
- 편집된 시간: 2016년 6월 29일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningFullAccess

설명: Amazon Machine Learning 리소스에 대한 전체 액세스 권한을 제공합니다.

AmazonMachineLearningFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 4월 9일, 17:25 UTC
- 편집된 시간: 2015년 4월 9일, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

설명: Amazon Machine Learning 모델의 실시간 엔드포인트를 생성하고 삭제할 수 있는 권한을 사용자에게 부여합니다.

AmazonMachineLearningManageRealTimeEndpointOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningManageRealTimeEndpointOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:32 UTC
- 편집된 시간: 2015년 4월 9일, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonMachineLearningManageRealTimeEndpointOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningReadOnlyAccess

설명: Amazon Machine Learning 리소스에 대한 읽기 전용 액세스를 제공합니다.

AmazonMachineLearningReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:40 UTC
- 편집된 시간: 2015년 4월 9일, 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "machinelearning:Describe*",
      "machinelearning:Get*"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

설명: 사용자에게 Amazon Machine Learning 실시간 예측을 요청할 수 있는 권한을 부여합니다.

AmazonMachineLearningRealTimePredictionOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningRealTimePredictionOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:44 UTC
- 편집된 시간: 2015년 4월 9일, 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

설명: 기계 학습이 Redshift 데이터 소스의 Redshift 클러스터 및 S3 스테이징 위치를 구성하고 사용할 수 있도록 합니다.

AmazonMachineLearningRoleforRedshiftDataSourceV3 [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningRoleforRedshiftDataSourceV3를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 24일, 18:00 UTC
- 편집된 시간: 2020년 6월 24일, 18:00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMacieFullAccess

설명: Amazon Macie에 대한 전체 액세스 권한을 제공합니다.

AmazonMacieFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 14:54 UTC

- 편집된 시간: 2022년 7월 1일, 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMacieHandshakeRole

설명: Amazon Macie의 서비스 연결 역할을 생성할 권한을 부여합니다.

AmazonMacieHandshakeRole [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieHandshakeRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 6월 28일, 15:46 UTC
- 편집된 시간: 2018년 6월 28일, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AWSServiceName" : "macie.amazonaws.com"
      }
    }
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMacieReadOnlyAccess

설명: Amazon Macie에 대한 읽기 전용 액세스를 제공합니다.

AmazonMacieReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 15일, 21:50 UTC
- 편집된 시간: 2023년 6월 15일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMacieServiceRole

설명: 데이터 분석을 가능하게 하기 위해 Macie에게 계정의 리소스 종속성에 대한 읽기 전용 액세스 권한을 부여합니다.

AmazonMacieServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 14:53 UTC
- 편집된 시간: 2017년 8월 14일, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMacieServiceRolePolicy

설명: Amazon Macie의 서비스 연결 역할

AmazonMacieServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 19일, 22:17 UTC
- 편집된 시간: 2022년 5월 19일, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
  ]
}

```



```

    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonManagedBlockchainConsoleFullAccess

설명: 다음을 통해 Amazon Managed Blockchain에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonManagedBlockchainConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonManagedBlockchainConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 29일, 21:23 UTC
- 편집된 시간: 2019년 4월 29일, 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "managedblockchain:*",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:CreateVpcEndpoint",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonManagedBlockchainFullAccess

설명: Amazon Managed Blockchain에 대한 전체 액세스 권한을 제공합니다.

AmazonManagedBlockchainFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonManagedBlockchainFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 29일, 21:39 UTC

- 편집된 시간: 2019년 4월 29일, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonManagedBlockchainReadOnlyAccess

설명: Amazon Managed Blockchain에 대한 읽기 전용 액세스를 제공합니다.

AmazonManagedBlockchainReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonManagedBlockchainReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 30일, 18:17 UTC
- 편집된 시간: 2019년 4월 30일, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonManagedBlockchainServiceRolePolicy

설명: Amazon Managed Blockchain에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 사용할 수 있도록 합니다.

AmazonManagedBlockchainServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 1월 17일, 19:51 UTC
- 편집된 시간: 2020년 1월 17일, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMCSFullAccess

설명: Amazon 관리형 아파치 카산드라 서비스에 대한 전체 액세스 권한 제공

AmazonMCSFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMCSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 13:45 UTC
- 편집된 시간: 2020년 4월 17일, 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMCSReadOnlyAccess

설명: Amazon 관리형 Apache Cassandra 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonMCSReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMCSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 13:46 UTC
- 편집된 시간: 2020년 4월 17일, 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMechanicalTurkFullAccess

설명: Amazon Mechanical Turk의 모든 API에 대한 전체 액세스 권한을 제공합니다.

AmazonMechanicalTurkFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMechanicalTurkFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 11일, 19:08 UTC
- 편집된 시간: 2015년 12월 11일, 19:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMechanicalTurkReadOnly

설명: Amazon Mechanical Turk의 읽기 전용 API에 대한 액세스를 제공합니다.

AmazonMechanicalTurkReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMechanicalTurkReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 11일, 19:08 UTC

- 편집된 시간: 2019년 9월 25일, 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMemoryDBFullAccess

설명: 를 통해 Amazon MemoryDB에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonMemoryDBFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMemoryDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 8일, 19:24 UTC
- 편집된 시간: 2021년 10월 8일, 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMemoryDBReadOnlyAccess

설명: 를 통해 Amazon MemoryDB에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonMemoryDBReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMemoryDBReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 8일, 19:27 UTC
- 편집된 시간: 2021년 10월 8일, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMobileAnalyticsFinancialReportAccess

설명: 모든 애플리케이션 리소스의 재무 데이터를 포함한 모든 보고서에 대한 읽기 전용 액세스를 제공합니다.

AmazonMobileAnalyticsFinancialReportAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsFinancialReportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMobileAnalyticsFullAccess

설명: 모든 애플리케이션 리소스에 대한 전체 액세스를 제공합니다.

AmazonMobileAnalyticsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMobileAnalyticsNon-financialReportAccess

설명: 모든 애플리케이션 리소스의 비재무 보고서에 대한 읽기 전용 액세스를 제공합니다.

AmazonMobileAnalyticsNon-financialReportAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsNon-financialReportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMobileAnalyticsWriteOnlyAccess

설명: 모든 애플리케이션 리소스에 대한 이벤트 데이터를 넣을 수 있는 쓰기 전용 액세스 권한을 제공합니다. (SDK 통합에 권장)

AmazonMobileAnalyticsWriteOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsWriteOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMonitronFullAccess

설명: Amazon Monitron을 관리할 수 있는 전체 액세스 권한을 제공합니다.

AmazonMonitronFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMonitronFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 2일, 22:40 UTC
- 편집된 시간: 2022년 6월 8일, 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMQApiFullAccess

설명: API/SDK를 통해 AmazonMQ에 완전히 액세스할 수 있습니다.

AmazonMQApiFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMQApiFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 18일, 20:31 UTC
- 편집된 시간: 2020년 11월 4일, 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMQApiReadOnlyAccess

설명: API/SDK를 통해 AmazonMQ에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonMQApiReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMQApiReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 18일, 20:31 UTC
- 편집된 시간: 2018년 12월 18일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMQFullAccess

설명: 를 통해 AmazonMQ에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonMQFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMQFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 11월 28일, 15:28 UTC
- 편집된 시간: 2020년 11월 4일, 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMQReadOnlyAccess

설명: 를 통해 AmazonMQ에 대한 읽기 전용 액세스 권한을 제공합니다. AWS Management Console

AmazonMQReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonMQReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 11월 28일, 15:30 UTC
- 편집된 시간: 2017년 11월 28일, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMQServiceRolePolicy

설명: AWS Amazon MQ용 서비스 연결 역할 정책

AmazonMQServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 4일, 16:07 UTC
- 편집된 시간: 2020년 11월 4일, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMSKConnectReadOnlyAccess

설명: Amazon MSK Connect에 대한 읽기 전용 액세스를 제공합니다.

AmazonMSKConnectReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMSKConnectReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 20일, 10:18 UTC
- 편집된 시간: 2021년 10월 18일, 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMSKFullAccess

설명: Amazon MSK에 대한 전체 액세스 권한과 종속성에 필요한 기타 권한을 제공하십시오.

AmazonMSKFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMSKFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 14일, 22:07 UTC
- 편집된 시간: 2023년 10월 18일, 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMSKReadOnlyAccess

설명: Amazon MSK에 대한 읽기 전용 액세스 권한 제공

AmazonMSKReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMSKReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 14일, 22:28 UTC
- 편집된 시간: 2019년 1월 14일, 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonMWAAServiceRolePolicy

설명: Apache Airflow용 Amazon 관리형 워크플로에서 사용하는 서비스 연결 역할입니다.

AmazonMWAAServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 24일, 14:13 UTC
- 편집된 시간: 2022년 11월 17일, 00:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonNimbleStudio-LaunchProfileWorker

설명: 이 정책은 Nimble Studio Launch Profile 작업자에게 필요한 리소스에 대한 액세스 권한을 부여합니다. 이 정책을 Nimble Studio Builder에서 생성된 EC2 인스턴스에 연결하세요.

AmazonNimbleStudio-LaunchProfileWorker [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonNimbleStudio-LaunchProfileWorker를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 28일, 04:47 UTC
- 편집된 시간: 2021년 4월 28일, 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonNimbleStudio-StudioAdmin

설명: 이 정책은 스튜디오 관리자와 관련된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스 권한을 부여합니다. 이 정책을 스튜디오와 연관된 관리자 역할에 연결하세요.

AmazonNimbleStudio-StudioAdmin [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonNimbleStudio-StudioAdmin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 28일, 04:47 UTC
- 편집된 시간: 2023년 9월 22일, 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonNimbleStudio-StudioUser

설명: 이 정책은 스튜디오 사용자와 관련된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스 권한을 부여합니다. 이 정책을 스튜디오와 연관된 사용자 역할에 연결하세요.

AmazonNimbleStudio-StudioUser [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonNimbleStudio-StudioUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 28일, 04:48 UTC
- 편집된 시간: 2023년 9월 22일, 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOmicsFullAccess

설명: Amazon Omics에 대한 전체 액세스 권한 및 기타 필수 AWS 서비스기능을 제공합니다. 이 정책을 통해 사용자는 사용자의 AWS 계정외부 리소스에 액세스하기 위한 RAM 공유 초대를 보고 수락할 수 있습니다.

AmazonOmicsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOmicsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2023년 2월 24일, 00:59 UTC
- 편집된 시간: 2023년 2월 24일, 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOmicsReadOnlyAccess

설명: Amazon Omics에 대한 읽기 전용 액세스 권한 제공

AmazonOmicsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOmicsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 29일, 04:17 UTC
- 편집된 시간: 2022년 11월 29일, 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOneEnterpriseFullAccess

설명: 이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 대한 액세스를 허용하는 관리자 권한을 부여합니다.

AmazonOneEnterpriseFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOneEnterpriseFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 28일 04:58 UTC
- 편집 시간: 2023년 11월 28일, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOneEnterpriseInstallerAccess

설명: 이 정책은 장치 설치 및 활성화를 허용하는 제한된 읽기 및 쓰기 권한을 부여합니다.

AmazonOneEnterpriseInstallerAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOneEnterpriseInstallerAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일 05:00 UTC
- 편집 시간: 2023년 11월 28일 05:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ]
    }
  ]
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOneEnterpriseReadOnlyAccess

설명: 이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 읽기 전용 권한을 부여합니다.

AmazonOneEnterpriseReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOneEnterpriseReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일 04:59 UTC
- 편집 시간: 2023년 11월 28일, 04:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchDashboardsServiceRolePolicy

설명: Amazon OpenSearch Dashboard 서비스에 대한 액세스를 제공하여 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있습니다. CloudWatch

AmazonOpenSearchDashboardsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 작성 시간: 2023년 12월 22일 19:38 UTC
- 편집 시간: 2023년 12월 22일 19:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

설명: OpenSearch DirectQuery 서비스가 AWS Glue API에 액세스하여 사용자를 대신하여 리소스를 생성할 수 있도록 허용합니다.

AmazonOpenSearchDirectQueryGlueCreateAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchDirectQueryGlueCreateAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 5월 6일 12:24 UTC
- 편집 시간: 2024년 5월 6일 12시 24분 (UTC)
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",

```

```
    "glue:CreateTable",
    "glue:BatchCreatePartition"
  ],
  "Resource" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchIngestionFullAccess

설명: Amazon OpenSearch Ingestion이 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

AmazonOpenSearchIngestionFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchIngestionFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 26일, 18:11 UTC
- 편집된 시간: 2023년 4월 26일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchIngestionReadOnlyAccess

설명: Amazon OpenSearch 통합 서비스에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonOpenSearchIngestionReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchIngestionReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 26일, 18:09 UTC
- 편집된 시간: 2023년 4월 26일, 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "osis:GetPipeline",
    "osis:GetPipelineChangeProgress",
    "osis:GetPipelineBlueprint",
    "osis:ListPipelineBlueprints",
    "osis:ListPipelines",
    "osis:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchIngestionServiceRolePolicy

설명: Amazon 통합 서비스가 OpenSearch 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

AmazonOpenSearchIngestionServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 18일, 16:49 UTC
- 편집된 시간: 2022년 11월 18일, 16:49 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


}

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchServerlessServiceRolePolicy

설명: Amazon OpenSearch Serverless가 사용자를 대신하여 CloudWatch API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용하십시오.

AmazonOpenSearchServerlessServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 24일, 19:50 UTC
- 편집된 시간: 2022년 11월 24일, 19:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

{

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchServiceCognitoAccess

설명: Amazon Cognito 구성 서비스에 대한 액세스를 제공합니다.

AmazonOpenSearchServiceCognitoAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchServiceCognitoAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 2일, 06:31 UTC
- 편집된 시간: 2021년 12월 20일, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchServiceFullAccess

설명: Amazon OpenSearch 서비스 구성 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonOpenSearchServiceFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchServiceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 8일, 05:33 UTC
- 편집된 시간: 2021년 9월 8일, 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchServiceReadOnlyAccess

설명: Amazon OpenSearch 서비스 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

AmazonOpenSearchServiceReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchServiceReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 9월 8일, 05:38 UTC
- 편집된 시간: 2021년 9월 8일, 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonOpenSearchServiceRolePolicy

설명: Amazon OpenSearch Service가 사용자를 대신하여 EC2 네트워킹 API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용하십시오.

AmazonOpenSearchServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 26일, 09:27 UTC
- 편집된 시간: 2023년 10월 23일, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPersonalizeFullAccess

설명: AWS Management Console 및 SDK를 통해 Amazon Personalize에 대한 전체 액세스 권한을 제공합니다. 또한 관련 서비스 (예: S3, CloudWatch) 에 대한 선택적 액세스를 제공합니다.

AmazonPersonalizeFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPersonalizeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 12월 4일, 22:24 UTC
- 편집된 시간: 2019년 5월 30일, 23:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPollyFullAccess

설명: Amazon Polly 서비스 및 리소스에 대한 전체 액세스 권한을 부여합니다.

AmazonPollyFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPollyFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 18:59 UTC
- 편집된 시간: 2016년 11월 30일, 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPollyReadOnlyAccess

설명: Amazon Polly 리소스에 대한 읽기 전용 액세스 권한을 부여합니다.

AmazonPollyReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonPollyReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 18:59 UTC
- 편집된 시간: 2018년 7월 17일, 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPrometheusConsoleFullAccess

설명: 콘솔에서 AWS 관리형 Prometheus 리소스에 대한 전체 액세스 권한을 부여합니다. AWS

AmazonPrometheusConsoleFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:11 UTC
- 편집된 시간: 2022년 10월 24일, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPrometheusFullAccess

설명: AWS 관리형 Prometheus 리소스에 대한 전체 액세스 권한을 부여합니다.

AmazonPrometheusFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:10 UTC
- 편집 시간: 2023년 11월 26일 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPrometheusQueryAccess

설명: AWS 관리형 Prometheus 리소스에 대해 쿼리를 실행할 수 있는 액세스 권한을 부여합니다.

AmazonPrometheusQueryAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusQueryAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 19일, 01:02 UTC
- 편집된 시간: 2020년 12월 19일, 01:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPrometheusRemoteWriteAccess

설명: AWS 관리형 Prometheus 작업 영역에 대한 쓰기 전용 액세스 권한을 부여합니다.

AmazonPrometheusRemoteWriteAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusRemoteWriteAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 19일, 01:04 UTC
- 편집된 시간: 2020년 12월 19일, 01:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Action" : [
      "aps:RemoteWrite"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonPrometheusScrapingServiceRolePolicy

설명: Prometheus 컬렉터용 아마존 매니지드 서비스에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

AmazonPrometheusScrapingServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2023년 11월 26일 14:19 UTC
- 편집 시간: 2024년 4월 26일 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapingServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    }
  ]
}
```



```

    }
  },
  {
    "Sid" : "TagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "Null" : {
        "aws:RequestTag/AMPAgentlessScrapper" : "false"
      }
    }
  },
  {
    "Sid" : "ENIUpdating",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AMPAgentlessScrapper" : "false"
      }
    }
  },
  {
    "Sid" : "EKSAccess",
    "Effect" : "Allow",
    "Action" : "eks:DescribeCluster",
    "Resource" : "arn:aws:eks:*:*:cluster/*"
  },
  {
    "Sid" : "DeleteEKSAccessEntry",
    "Effect" : "Allow",
    "Action" : "eks:DeleteAccessEntry",
    "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
}

```

```

    },
    "ArnLike" : {
      "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
    }
  },
  {
    "Sid" : "APSWriting",
    "Effect" : "Allow",
    "Action" : "aps:RemoteWrite",
    "Resource" : "arn:aws:aps:*:*:workspace/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonQFullAccess

설명: Amazon Q와의 상호 작용이 가능하도록 전체 액세스 권한을 제공합니다.

AmazonQFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일 16:00 UTC

- 편집 시간: 2024년 4월 29일 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonQLDBConsoleFullAccess

설명: 를 통해 Amazon QLDB에 대한 전체 액세스 권한을 제공합니다. AWS Management Console AmazonQLDBConsoleFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQLDBConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:24 UTC
- 편집된 시간: 2022년 11월 4일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonQLDBFullAccess

설명: 서비스 API를 통해 Amazon QLDB에 대한 전체 액세스를 제공합니다.

AmazonQLDBFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQLDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:23 UTC

- 편집된 시간: 2022년 11월 4일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonQLDBReadOnly

설명: Amazon QLDB에 대한 읽기 전용 액세스를 제공합니다.

AmazonQLDBReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQLDBReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:19 UTC
- 편집된 시간: 2021년 7월 2일, 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSBetaServiceRolePolicy

설명: Amazon RDS가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonRDSBetaServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 2일, 19:41 UTC
- 편집된 시간: 2022년 12월 14일, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSCustomInstanceProfileRolePolicy

설명: Amazon RDS Custom이 EC2 인스턴스 프로필을 통해 다양한 자동화 작업 및 데이터베이스 관리 작업을 수행할 수 있도록 합니다.

AmazonRDSCustomInstanceProfileRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSCustomInstanceProfileRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 2월 27일 17:42 UTC
- 편집 시간: 2024년 2월 27일 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "cwlUploadPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutRetentionPolicy",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:CreateLogStream",
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
  },
  {
    "Sid" : "sendMessageToSqsQueuePermission",
    "Effect" : "Allow",
    "Action" : [
      "sqs:SendMessage",
      "sqs:ReceiveMessage",
      "sqs>DeleteMessage",
      "sqs:GetQueueUrl"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
      }
    }
  },
  {
    "Sid" : "managePrivateIpOnEniPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
      }
    }
  }
}
```

```

    }
  },
  {
    "Sid" : "kmsPermissionWithSecret",
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:do-
not-delete-rds-custom-*"
      },
      "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSCustomPreviewServiceRolePolicy

설명: Amazon RDS 사용자 지정 미리 보기 서비스 역할 정책

AmazonRDSCustomPreviewServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 8일, 21:44 UTC
- 편집된 시간: 2023년 9월 20일, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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" : "RequireImsv2",
  "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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSCustomServiceRolePolicy

설명: Amazon RDS Custom이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonRDSCustomServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 8일, 21:39 UTC

- 편집 시간: 2024년 4월 19일 오후 5시 15분 (UTC)
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
```

```

    "ec2:DescribeTransitGatewayMulticastDomains",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ecc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation",
    "ec2:TerminateInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:RebootInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {

```



```

        "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
        ]
    }
},
{
    "Sid" : "ecc1scoping2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ecc1scoping3",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle-rac"
            ]
        }
    }
},

```

```

{
  "Sid" : "eccRunInstances1",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group/*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {

```

```

    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac",
        "custom-oracle"
      ]
    }
  },
  {
    "Sid" : "eccModifyInstanceAttribute1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyInstanceAttribute"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-sqlserver"
        ],
        "ec2:Attribute" : "InstanceType"
      }
    }
  },
  {
    "Sid" : "RequireImdsV2",
    "Effect" : "Deny",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringNotEquals" : {
        "ec2:MetadataHttpTokens" : "required"
      },
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances3keyPair1",

```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:DeleteKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccKeyPair2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccNetworkInterface1",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {

```

```

        "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
        ]
    }
}
},
{
    "Sid" : "eccNetworkInterface2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
    ]
},
{
    "Sid" : "eccNetworkInterface3",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "eccCreateTag1",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    ]
}

```

```

    }
  }
},
{
  "Sid" : "eccCreateTag2",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ],
      "ec2:CreateAction" : [
        "CreateKeyPair",
        "RunInstances",
        "CreateNetworkInterface",
        "CreateVolume",
        "CreateSnapshot",
        "CreateSnapshots",
        "CopySnapshot",
        "AllocateAddress"
      ]
    }
  }
},
{
  "Sid" : "eccVolume1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",

```

```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "eccVolume2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVolume",
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:ModifyVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume4snapshot1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume",
```

```

    "ec2:DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopySnapshot",
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",

```



```

        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "eccSnapshot4",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshot",
    "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-sqlserver"
            ]
        }
    }
},
{
    "Sid" : "iam1",
    "Effect" : "Allow",
    "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
    ],
    "Resource" : "*"
},
{
    "Sid" : "iam2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam:*:*:role/AWSRDSCustom*",
        "arn:aws:iam:*:*:role/service-role/AWSRDSCustom*"
    ]
},

```

```
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "cloudtrail1",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:GetTrailStatus"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "cw1",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:EnableAlarmActions",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "cw2",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:TagResource"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
```

```
        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "cw3",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
},
{
    "Sid" : "ssm1",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ssm:*:*:document/*"
},
{
    "Sid" : "ssm2",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ssm3",
    "Effect" : "Allow",
    "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
}
```

```
  },
  {
    "Sid" : "ssm4",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter",
      "ssm:AddTagsToResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ssm5",
    "Effect" : "Allow",
    "Action" : [
      "ssm>DeleteParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eb1",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:TagResource"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",

```

```
        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "eb2",
    "Effect" : "Allow",
    "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "eb3",
    "Effect" : "Allow",
    "Action" : [
        "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "events:ManagedBy" : [
                "custom.rds.amazonaws.com"
            ]
        }
    }
},
},
```

```
{
  "Sid" : "eb4",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:EnableRule",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "events:ManagedBy" : [
        "custom.rds.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "eb5",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
},
{
  "Sid" : "secretmanager1",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:TagResource",
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "secretmanager2",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "sqs1",
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs:TagQueue"
    ],
    "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-sqlserver"
        ]
      }
    }
  },
  {
    "Sid" : "sqs2",
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:SendMessage",
```

```

    "sqs:ReceiveMessage",
    "sqs:DeleteMessage",
    "sqs:DeleteQueue"
  ],
  "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-sqlserver"
      ]
    }
  }
},
{
  "Sid" : "servicequota1",
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSDDataFullAccess

설명: RDS 데이터 API, RDS 데이터베이스 자격 증명을 위한 비밀 저장소 API 및 DB 콘솔 쿼리 관리 API를 사용하여 의 Aurora 서버리스 클러스터에서 SQL 문을 실행할 수 있는 전체 액세스 권한을 허용합니다. AWS 계정

AmazonRDSDDataFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSDDataFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 20일, 21:29 UTC
- 편집된 시간: 2019년 11월 20일, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSDirectoryServiceAccess

설명: 도메인에 조인된 SQL Server DB 인스턴스의 경우 RDS가 고객을 대신하여 Directory Service Managed AD에 액세스할 수 있도록 허용합니다.

AmazonRDSDirectoryServiceAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSDirectoryServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 26일, 02:02 UTC
- 편집된 시간: 2019년 5월 15일, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSEnhancedMonitoringRole

설명: RDS용 Cloudwatch의 향상된 모니터링에 대한 액세스를 제공합니다.

AmazonRDSEnhancedMonitoringRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSEnhancedMonitoringRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 11일, 19:58 UTC
- 편집된 시간: 2015년 11월 11일, 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSFullAccess

설명: 를 통해 Amazon RDS에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonRDSFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 8월 17일, 23:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSPerformanceInsightsFullAccess

설명: 를 통해 RDS Performance Insights에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonRDSPerformanceInsightsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSPerformanceInsightsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 15일, 23:41 UTC
- 편집된 시간: 2023년 10월 23일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSPerformanceInsightsReadOnly

설명: RDS Performance Insights의 읽기 전용 정책

AmazonRDSPerformanceInsightsReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSPerformanceInsightsReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 5일, 00:02 UTC
- 편집된 시간: 2023년 10월 23일, 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSPreviewServiceRolePolicy

설명: Amazon RDS 프리뷰 서비스 역할 정책

AmazonRDSPreviewServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 31일, 18:02 UTC
- 편집된 시간: 2023년 10월 4일, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSReadOnlyAccess

설명: 를 통해 Amazon RDS에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonRDSReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 4월 14일, 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRDSServiceRolePolicy

설명: Amazon RDS가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AmazonRDSServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 1월 8일, 18:17 UTC
- 편집 시간: 2024년 1월 19일 15:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftAllCommandsFullAccess

설명: 이 정책에는 Amazon Redshift에서 데이터를 복사, 로드, 언로드, 쿼리 및 분석하기 위한 SQL 명령을 실행할 수 있는 권한이 포함되어 있습니다. 이 정책은 또한 Amazon S3, Amazon CloudWatch 로그 SageMaker, Amazon 또는 AWS Glue와 같은 관련 서비스에 대해 선택된 명령문을 실행할 수 있는 권한을 부여합니다.

AmazonRedshiftAllCommandsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftAllCommandsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 4일, 00:48 UTC
- 편집된 시간: 2021년 11월 25일, 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
]

```

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftDataFullAccess

설명: 이 정책은 Amazon Redshift 데이터 API에 대한 전체 액세스를 제공합니다. 이 정책은 다른 필수 서비스에 대한 범위 지정된 액세스 권한도 부여합니다.

AmazonRedshiftDataFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftDataFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 9일, 19:23 UTC
- 편집된 시간: 2023년 4월 7일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}

```


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftFullAccess

설명: 를 통해 Amazon Redshift에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonRedshiftFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2022년 7월 7일, 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftQueryEditor

설명: Amazon Redshift 쿼리 편집기에 대한 전체 액세스 권한과 를 통해 저장된 쿼리에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonRedshiftQueryEditor [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditor를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 4일, 22:50 UTC
- 편집된 시간: 2021년 2월 16일, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftQueryEditorV2FullAccess

설명: Amazon Redshift 쿼리 편집기 V2 작업 및 리소스에 대한 전체 액세스 권한을 부여합니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고, AWS KMS에서 키와 별칭을 읽고, Secrets Manager에서 쿼리 편집기 V2 비밀을 관리할 수 있는 권한이 포함됩니다. AWS

AmazonRedshiftQueryEditorV2FullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:06 UTC
- 편집 시간: 2024년 2월 21일 17:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftQueryEditorV2NoSharing

설명: 리소스를 공유하지 않고도 Amazon Redshift 쿼리 편집기 V2를 사용할 수 있는 기능을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 업데이트하고, 삭제할 수만 있고 공유할 수는 없습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

AmazonRedshiftQueryEditorV2NoSharing [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2NoSharing를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:18 UTC
- 편집 시간: 2024년 2월 21일 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftQueryEditorV2ReadSharing

설명: 리소스를 제한적으로 공유하여 Amazon Redshift 쿼리 편집기 V2를 사용할 수 있는 권한을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 쓰고, 공유할 수 있습니다. 부여된 보안 주체는 팀과 공유된 리소스를 읽을 수 있지만 업데이트할 수는 없습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

AmazonRedshiftQueryEditorV2ReadSharing [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2ReadSharing를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:22 UTC

- 편집 시간: 2024년 2월 21일 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
    }
  }
}

```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

설명: 리소스를 공유하여 Amazon Redshift 쿼리 편집기 V2를 사용할 수 있는 권한을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 쓰고, 공유할 수 있습니다. 부여된 보안 주체는 팀과 공유하는 리소스를 읽고 업데이트할 수 있습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

AmazonRedshiftQueryEditorV2ReadWriteSharing [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2ReadWriteSharing를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:25 UTC
- 편집 시간: 2024년 2월 21일 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",
      "sqlworkbench>ListTabs",
      "sqlworkbench:UpdateFolder",
      "sqlworkbench>ListRedshiftClusters",
      "sqlworkbench:DriverExecute",
      "sqlworkbench>ListTaggedResources",
      "sqlworkbench>ListQueryExecutionHistory",
      "sqlworkbench:GetQueryExecutionHistory",
      "sqlworkbench>ListNotebooks",
      "sqlworkbench:GetSchemaInference",
      "sqlworkbench:GetAutocompletionMetadata",
      "sqlworkbench:GetAutocompletionResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateConnection",
      "sqlworkbench:CreateSavedQuery",
      "sqlworkbench:CreateChart",
      "sqlworkbench:CreateNotebook",
      "sqlworkbench:DuplicateNotebook",

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:user}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:DeleteChart",
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench:DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookCell",
    "sqlworkbench:DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench:DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
  ]
}

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-resource-owner"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:DuplicateNotebook",
  ]
}

```

```

    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:UntagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
}
]

```


}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftReadOnlyAccess

설명: 를 통해 Amazon Redshift에 대한 읽기 전용 액세스 권한을 제공합니다. AWS Management Console

AmazonRedshiftReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 2월 8일 00:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRedshiftServiceLinkedRolePolicy

설명: Amazon Redshift가 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

AmazonRedshiftServiceLinkedRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 18일, 19:19 UTC
- 편집 시간: 2024년 3월 15일 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    ]
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRekognitionCustomLabelsFullAccess

설명: 이 정책은 Amazon Rekognition 사용자 지정 레이블 기능에 필요한 인식 및 s3 권한을 지정합니다.

AmazonRekognitionCustomLabelsFullAccess관리형 [AWS 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRekognitionCustomLabelsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 8일, 19:18 UTC
- 편집된 시간: 2022년 8월 16일, 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRekognitionFullAccess

설명: 모든 아마존 Rekognition API에 대한 액세스

AmazonRekognitionFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRekognitionFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 14:40 UTC
- 편집된 시간: 2016년 11월 30일, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "rekognition:*"
  ],
  "Resource" : "*"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRekognitionReadOnlyAccess

설명: 모든 읽기 인식 API에 대한 액세스

AmazonRekognitionReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRekognitionReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 14:58 UTC
- 편집된 시간: 2023년 11월 8일, 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRekognitionServiceRole

설명: Rekognition이 사용자를 대신하여 서비스를 호출할 수 있도록 AWS 합니다.

AmazonRekognitionServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRekognitionServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 29일, 16:52 UTC
- 편집된 시간: 2017년 11월 29일, 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53AutoNamingFullAccess

설명: 모든 Route 53 자동 이름 지정 작업에 대한 전체 액세스 권한을 제공합니다.

AmazonRoute53AutoNamingFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53AutoNamingFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 1월 18일, 18:40 UTC
- 편집된 시간: 2018년 1월 18일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53AutoNamingReadOnlyAccess

설명: 모든 Route 53 자동 이름 지정 작업에 대한 읽기 전용 액세스를 제공합니다.

AmazonRoute53AutoNamingReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53AutoNamingReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 1월 18일, 03:02 UTC
- 편집된 시간: 2018년 1월 18일, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53AutoNamingRegistrantAccess

설명: Route 53 자동 이름 지정 작업에 등록자 수준의 액세스 권한을 제공합니다.

AmazonRoute53AutoNamingRegistrantAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53AutoNamingRegistrantAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 12일, 22:33 UTC
- 편집된 시간: 2018년 3월 12일, 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
```

```

        "*"
    ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53DomainsFullAccess

설명: 모든 Route53 도메인 작업 및 도메인 등록의 일환으로 호스팅 영역을 생성할 수 있는 호스팅 영역 생성에 대한 전체 액세스 권한을 제공합니다.

AmazonRoute53DomainsFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53DomainsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53DomainsReadOnlyAccess

설명: Route53 도메인 목록 및 작업에 대한 액세스를 제공합니다.

AmazonRoute53DomainsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53DomainsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53FullAccess

설명: 를 통해 모든 Amazon Route 53에 대한 전체 액세스를 제공합니다 AWS Management Console.

AmazonRoute53FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2018년 12월 20일, 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53ProfilesFullAccess

설명: 이 정책은 Amazon Route 53 프로파일 리소스에 대한 전체 액세스 권한을 부여합니다.

AmazonRoute53ProfilesFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ProfilesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 30일 18:30 UTC

- 편집 시간: 2024년 4월 30일 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53ProfilesReadOnlyAccess

설명: 이 정책은 Amazon Route 53 프로파일 리소스에 대한 읽기 전용 액세스 권한을 부여합니다.

AmazonRoute53ProfilesReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ProfilesReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 30일 18:29 UTC
- 편집 시간: 2024년 4월 30일 18:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53ReadOnlyAccess

설명: 를 통해 모든 Amazon Route 53에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonRoute53ReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 11월 15일, 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
```

```

        "*"
    ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryClusterFullAccess

설명: Amazon Route 53 복구 클러스터에 대한 전체 액세스 권한을 제공합니다.

AmazonRoute53RecoveryClusterFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryClusterFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:37 UTC
- 편집된 시간: 2021년 8월 18일, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

설명: Amazon Route 53 복구 클러스터에 대한 읽기 전용 액세스를 제공합니다.

AmazonRoute53RecoveryClusterReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryClusterReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 17:36 UTC
- 편집된 시간: 2022년 4월 1일, 17:37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryControlConfigFullAccess

설명: Amazon Route 53 복구 제어 구성에 대한 전체 액세스 권한을 제공합니다.

AmazonRoute53RecoveryControlConfigFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryControlConfigFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 17:48 UTC
- 편집된 시간: 2021년 8월 18일, 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

설명: Amazon Route 53 복구 제어 구성에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonRoute53RecoveryControlConfigReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryControlConfigReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:01 UTC
- 편집된 시간: 2023년 10월 18일, 17:15 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonRoute53RecoveryControlConfigReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryReadinessFullAccess

설명: Amazon Route 53 복구 준비에 대한 전체 액세스 권한을 제공합니다.

AmazonRoute53RecoveryReadinessFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryReadinessFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 16:45 UTC

- 편집된 시간: 2021년 8월 18일, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

설명: Amazon Route 53 복구 준비에 대한 읽기 전용 액세스를 제공합니다.

AmazonRoute53RecoveryReadinessReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryReadinessReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:11 UTC
- 편집된 시간: 2021년 11월 9일, 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53ResolverFullAccess

설명: Route 53 리졸버에 대한 전체 액세스 정책

AmazonRoute53ResolverFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ResolverFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 30일, 18:10 UTC
- 편집된 시간: 2020년 7월 17일, 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonRoute53ResolverReadOnlyAccess

설명: Route 53 리졸버에 대한 읽기 전용 정책

AmazonRoute53ResolverReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ResolverReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 30일, 18:11 UTC
- 편집된 시간: 2019년 9월 27일, 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ]
    }
  ],
}
```

```

    "Resource" : [
      "*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonS3FullAccess

설명: 를 통해 모든 버킷에 대한 전체 액세스를 제공합니다. AWS Management Console

AmazonS3FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2021년 9월 27일, 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonS3ObjectLambdaExecutionRolePolicy

설명: Amazon S3 AWS 객체 Lambda와 상호 작용할 수 있는 Lambda 함수 권한을 제공합니다. 또한 Lambda에 로그에 쓸 수 있는 권한을 부여합니다. CloudWatch

AmazonS3ObjectLambdaExecutionRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3ObjectLambdaExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 8월 18일, 10:07 UTC

- 편집된 시간: 2021년 8월 18일, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonS3OutpostsFullAccess

설명: 를 통해 Outposts의 Amazon S3에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonS3OutpostsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3OutpostsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 2일, 17:26 UTC
- 편집된 시간: 2020년 10월 2일, 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonS3OutpostsReadOnlyAccess

설명: 를 통해 Outposts의 Amazon S3에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonS3OutpostsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3OutpostsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 2일, 18:55 UTC
- 편집된 시간: 2020년 10월 2일, 18:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonS3ReadOnlyAccess

설명: 를 통해 모든 버킷에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonS3ReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 8월 10일, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

설명: AWS 서비스 카탈로그 서비스가 Amazon 제품 SageMaker 포트폴리오의 상품을 프로비저닝하는 데 사용하는 서비스 역할 정책입니다. CodePipeline,, CodeBuild CodeCommit, Glue 등을 포함한 일련의 관련 서비스에 권한을 부여합니다. CloudFormation

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 27일, 18:48 UTC
- 편집 시간: 2024년 6월 12일 18:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{  
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasAIServicesAccess

설명: Amazon SageMaker Canvas가 AI 서비스를 사용하여 바로 사용할 수 있는 AI 솔루션을 지원할 수 있는 권한을 제공합니다. Amazon SageMaker Canvas가 지원을 추가함에 따라 이 정책은 서비스에 대한 변경 권한을 더 추가합니다.

AmazonSageMakerCanvasAIServicesAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasAIServicesAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 23일, 22:36 UTC
- 편집 시간: 2023년 11월 29일 14:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasBedrockAccess

설명: 이 정책은 S3와 같은 다운스트림 서비스에 대한 액세스를 제공하여 SageMaker Canvas에서 Amazon Bedrock을 사용할 수 있는 권한을 부여합니다.

AmazonSageMakerCanvasBedrockAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasBedrockAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 2월 2일 18:37 UTC
- 편집 시간: 2024년 2월 2일 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasDataPrepFullAccess

설명: Canvas에서 데이터를 준비하기 위해 Amazon SageMaker 리소스 및 작업에 대한 전체 액세스 권한을 제공합니다. 이 정책은 또한 관련 서비스 (예: S3, IAM, KMS, RDS, 로그, Redshift, Athena, Glue, CloudWatch, Secrets Manager) 에 대한 선택적 액세스를 제공합니다. EventBridge 이 정책은 Amazon SageMaker 도메인/사용자 프로필 실행 역할에 연결되어야 합니다.

AmazonSageMakerCanvasDataPrepFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasDataPrepFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 10월 27일, 22:56 UTC
- 편집 시간: 2023년 12월 8일 02:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    }
  ]
}
```

```
},
{
  "Sid" : "SageMakerPipelineOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribePipeline",
    "sagemaker:CreatePipeline",
    "sagemaker:UpdatePipeline",
    "sagemaker>DeletePipeline",
    "sagemaker:StartPipelineExecution",
    "sagemaker>ListPipelineExecutionSteps",
    "sagemaker:DescribePipelineExecution"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
},
{
  "Sid" : "KMSListOperations",
  "Effect" : "Allow",
  "Action" : "kms:ListAliases",
  "Resource" : "*"
},
{
  "Sid" : "KMSOperations",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Sid" : "S3Operations",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3>DeleteObject",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:AbortMultipartUpload"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ],
  "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  },
  {
    "Sid" : "S3GetObjectOperation",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3:::*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      },
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "S3ListOperations",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMListOperations",
    "Effect" : "Allow",
    "Action" : "iam:ListRoles",
    "Resource" : "*"
  },
  {
    "Sid" : "IAMGetOperations",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/*"
  },
  {
    "Sid" : "IAMPassOperation",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
```

```
"Resource" : "arn:aws:iam::*:role/*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "sagemaker.amazonaws.com",
      "events.amazonaws.com"
    ]
  }
},
{
  "Sid" : "EventBridgePutOperation",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events::*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:PutTargets"
  ],
  "Resource" : "arn:aws:events::*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeTagBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:TagResource"
  ],
  "Resource" : "arn:aws:events::*:rule/*",
```

```
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
    "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
  }
},
{
  "Sid" : "EventBridgeListTagOperation",
  "Effect" : "Allow",
  "Action" : "events:ListTagsForResource",
  "Resource" : "*"
},
{
  "Sid" : "GlueOperations",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:SearchTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "EMROperations",
  "Effect" : "Allow",
  "Action" : [
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups"
  ],
  "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
},
{
  "Sid" : "EMRListOperation",
  "Effect" : "Allow",
  "Action" : "elasticmapreduce:ListClusters",
  "Resource" : "*"
},
{
```

```
"Sid" : "AthenaListDataCatalogOperation",
"Effect" : "Allow",
"Action" : "athena:ListDataCatalogs",
"Resource" : "*"
},
{
  "Sid" : "AthenaQueryExecutionOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution"
  ],
  "Resource" : "arn:aws:athena:*:*:workgroup/*"
},
{
  "Sid" : "AthenaDataCatalogOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : "arn:aws:athena:*:*:datacatalog/*"
},
{
  "Sid" : "RedshiftOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:DescribeStatement",
    "redshift-data:CancelStatement",
    "redshift-data:GetStatementResult"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RedshiftArnBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ],
  "Resource" : "arn:aws:redshift:*:*:cluster:*"
```

```

},
{
  "Sid" : "RedshiftGetCredentialsOperation",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentials",
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "SecretsManagerARNBasedOperation",
  "Effect" : "Allow",
  "Action" : "secretsmanager:CreateSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
},
{
  "Sid" : "SecretManagerTagBasedOperation",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",
  "Action" : "rds:DescribeDBInstances",
  "Resource" : "*"
},
{
  "Sid" : "LoggingOperation",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ]
}

```

```

    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasDirectDeployAccess

설명: Amazon SageMaker Canvas에서 Canvas를 통해 생성된 엔드포인트의 엔드포인트 세부 정보를 생성, 관리 및 볼 수 있도록 허용합니다. Amazon SageMaker Canvas에서 CloudWatch 엔드포인트 호출 지표를 검색할 수 있도록 허용합니다.

AmazonSageMakerCanvasDirectDeployAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasDirectDeployAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 6일, 18:11 UTC
- 편집된 시간: 2023년 10월 6일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasForecastAccess

설명: 이 정책은 Amazon Forecast에서 SageMaker Canvas를 사용하는 데 일반적으로 필요한 권한을 부여합니다.

AmazonSageMakerCanvasForecastAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasForecastAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 8월 24일, 20:04 UTC
- 편집된 시간: 2022년 8월 24일, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCanvasFullAccess

설명: Amazon SageMaker Canvas 리소스 및 작업에 대한 전체 액세스 권한을 제공합니다. 또한 이 정책은 관련 서비스 (예: S3, IAM, VPC, ECR, CloudWatch 로그, Redshift, Secrets Manager 및 Forecast)에 대한 선택적 액세스를 제공합니다. 이 정책은 Amazon SageMaker 도메인/사용자 프로필 실행 역할에 연결되어야 합니다.

AmazonSageMakerCanvasFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 9월 9일, 00:44 UTC

- 편집 시간: 2024년 1월 24일 22:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}

```

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerClusterInstanceRolePolicy

설명: 이 정책은 Amazon SageMaker Cluster를 사용하는 데 일반적으로 필요한 권한을 부여합니다.

AmazonSageMakerClusterInstanceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerClusterInstanceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 29일 15:11 UTC
- 편집 시간: 2023년 11월 29일 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerCoreServiceRolePolicy

설명: Amazon SageMaker Core 서비스의 서비스 연결 역할에 대한 관리형 정책

AmazonSageMakerCoreServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 21일, 21:40 UTC
- 편집된 시간: 2020년 12월 21일, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerEdgeDeviceFleetPolicy

설명: 기본 클라우드 연결을 사용하는 고객을 위해 SageMaker Edge가 디바이스 플릿을 생성하고 관리하는 데 필요한 권한을 제공합니다.

AmazonSageMakerEdgeDeviceFleetPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerEdgeDeviceFleetPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 8일, 16:17 UTC

- 편집된 시간: 2020년 12월 8일, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerFeatureStoreAccess

설명: Amazon SageMaker FeatureStore 기능 그룹의 오프라인 스토어를 활성화하는 데 필요한 권한을 제공합니다.

AmazonSageMakerFeatureStoreAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerFeatureStoreAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:24 UTC
- 편집된 시간: 2022년 12월 5일, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerFullAccess

설명: AWS Management Console 및 SageMaker SDK를 통해 Amazon에 대한 전체 액세스 권한을 제공합니다. 또한 관련 서비스 (예: S3, ECR, CloudWatch 로그) 에 대한 선택적 액세스를 제공합니다.

AmazonSageMakerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 13:07 UTC
- 편집 시간: 2024년 3월 29일 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

정책 버전

정책 버전: v26(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Sid" : "AllowAllNonAdminSageMakerActions",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:*",
      "sagemaker-geospatial:*"
    ],
    "NotResource" : [
      "arn:aws:sagemaker:*:*:domain/*",
      "arn:aws:sagemaker:*:*:user-profile/*",
      "arn:aws:sagemaker:*:*:app/*",
      "arn:aws:sagemaker:*:*:space/*",
      "arn:aws:sagemaker:*:*:flow-definition/*"
    ]
  },
  {
    "Sid" : "AllowAddTagsForSpace",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:AddTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "sagemaker:TaggingAction" : "CreateSpace"
      }
    }
  },
  {
    "Sid" : "AllowAddTagsForApp",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:AddTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:app/*"
    ]
  },
  {
    "Sid" : "AllowStudioActions",
    "Effect" : "Allow",

```

```

    "Action" : [
      "sagemaker:CreatePresignedDomainUrl",
      "sagemaker:DescribeDomain",
      "sagemaker:ListDomains",
      "sagemaker:DescribeUserProfile",
      "sagemaker:ListUserProfiles",
      "sagemaker:DescribeSpace",
      "sagemaker:ListSpaces",
      "sagemaker:DescribeApp",
      "sagemaker:ListApps"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAppActionsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  },
  {
    "Sid" : "AllowAppActionsForSharedSpaces",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition" : {
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Shared"
        ]
      }
    }
  }
]

```

```

    "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker:UpdateSpace",
      "sagemaker>DeleteSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  },
  {
    "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker:UpdateSpace",
      "sagemaker>DeleteSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private",
          "Shared"
        ]
      }
    }
  }
},
{
  "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker>CreateApp",
    "sagemaker>DeleteApp"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",

```



```

    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private"
        ]
      }
    }
  },
  {
    "Sid" : "AllowFlowDefinitionActions",
    "Effect" : "Allow",
    "Action" : "sagemaker:*",
    "Resource" : [
      "arn:aws:sagemaker:*:*:flow-definition/*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "sagemaker:WorkteamType" : [
          "private-crowd",
          "vendor-crowd"
        ]
      }
    }
  }
},
{
  "Sid" : "AllowAWSServiceActions",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",

```

```
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:PutMetricAlarm",
"cloudwatch:PutMetricData",
"codecommit:BatchGetRepositories",
"codecommit:CreateRepository",
"codecommit:GetRepository",
"codecommit:List*",
"cognito-idp:AdminAddUserToGroup",
"cognito-idp:AdminCreateUser",
"cognito-idp:AdminDeleteUser",
"cognito-idp:AdminDisableUser",
"cognito-idp:AdminEnableUser",
"cognito-idp:AdminRemoveUserFromGroup",
"cognito-idp:CreateGroup",
"cognito-idp:CreateUserPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp:CreateUserPoolDomain",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:List*",
"cognito-idp:UpdateUserPool",
"cognito-idp:UpdateUserPoolClient",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateVpcEndpoint",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:CreateRepository",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
```

```
"ecr:StartImageScan",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"fsx:DescribeFileSystems",
"glue:CreateJob",
"glue>DeleteJob",
"glue:GetJob*",
"glue:GetTable*",
"glue:GetWorkflowRun",
"glue:ResetJobBookmark",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:UpdateJob",
"groundtruthlabeling:*",
"iam:ListRoles",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogDelivery",
"logs:Describe*",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:PutResourcePolicy",
"logs:UpdateLogDelivery",
"robomaker:CreateSimulationApplication",
"robomaker:DescribeSimulationApplication",
"robomaker>DeleteSimulationApplication",
"robomaker:CreateSimulationJob",
"robomaker:DescribeSimulationJob",
"robomaker:CancelSimulationJob",
"secretsmanager:ListSecrets",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"sns:ListTopics",
>tag:GetResources"
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowECRActions",
    "Effect" : "Allow",
    "Action" : [
      "ecr:SetRepositoryPolicy",
      "ecr:CompleteLayerUpload",
      "ecr:BatchDeleteImage",
      "ecr:UploadLayerPart",
      "ecr>DeleteRepositoryPolicy",
      "ecr:InitiateLayerUpload",
      "ecr>DeleteRepository",
      "ecr:PutImage"
    ],
    "Resource" : [
      "arn:aws:ecr:*:*:repository/*sagemaker*"
    ]
  },
  {
    "Sid" : "AllowCodeCommitActions",
    "Effect" : "Allow",
    "Action" : [
      "codecommit:GitPull",
      "codecommit:GitPush"
    ],
    "Resource" : [
      "arn:aws:codecommit:*:*:*sagemaker*",
      "arn:aws:codecommit:*:*:*SageMaker*",
      "arn:aws:codecommit:*:*:*Sagemaker*"
    ]
  },
  {
    "Sid" : "AllowCodeBuildActions",
    "Action" : [
      "codebuild:BatchGetBuilds",
      "codebuild:StartBuild"
    ],
    "Resource" : [
      "arn:aws:codebuild:*:*:project/sagemaker*",
      "arn:aws:codebuild:*:*:build/*"
    ],
    "Effect" : "Allow"
  }
```

```
},
{
  "Sid" : "AllowStepFunctionsActions",
  "Action" : [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
    "arn:aws:states:*:*:execution:*sagemaker*:*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowSecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
  ]
},
{
  "Sid" : "AllowReadOnlySecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/SageMaker" : "true"
    }
  }
},
{
  "Sid" : "AllowServiceCatalogProvisionProduct",
```

```

    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:ProvisionProduct"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:TerminateProvisionedProduct",
      "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "servicecatalog:userLevel" : "self"
      }
    }
  },
  {
    "Sid" : "AllowS3ObjectActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*",
      "arn:aws:s3::*aws-glue*"
    ]
  },
  {
    "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*"
    ]
  }

```

```
    ],
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      }
    }
  },
  {
    "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*"
    ],
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
      }
    }
  },
  {
    "Sid" : "AllowS3BucketActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:GetBucketCors",
      "s3:PutBucketCors"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowS3BucketACL",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketAcl",
      "s3:PutObjectAcl"
    ],
    "Resource" : [
      "arn:aws:s3:::*SageMaker*",

```

```

    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ]
},
{
  "Sid" : "AllowLambdaInvokeFunction",
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda::*:function:*SageMaker*",
    "arn:aws:lambda::*:function:*sagemaker*",
    "arn:aws:lambda::*:function:*Sagemaker*",
    "arn:aws:lambda::*:function:*LabelingFunction*"
  ]
},
{
  "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "robomaker.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowSNSActions",
  "Effect" : "Allow",
  "Action" : [

```



```

    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sagemaker*"
  ]
},
{
  "Sid" : "AllowPassRoleForSageMakerRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com",
        "robomaker.amazonaws.com",
        "states.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AllowPassRoleToSageMaker",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "sagemaker.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowAthenaActions",
  "Effect" : "Allow",
  "Action" : [

```

```

    "athena:ListDataCatalogs",
    "athena:ListDatabases",
    "athena:ListTableMetadata",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowGlueCreateTable",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
    "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "AllowGlueUpdateTable",
  "Effect" : "Allow",
  "Action" : [
    "glue:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/sagemaker_featurestore"
  ]
},
{
  "Sid" : "AllowGlueDeleteTable",
  "Effect" : "Allow",
  "Action" : [
    "glue>DeleteTable"
  ],
  "Resource" : [

```

```

    "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "AllowGlueGetTablesAndDatabases",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "AllowGlueGetAndCreateDatabase",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue:GetDatabase"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/sagemaker_featurestore",
    "arn:aws:glue:*:*:database/sagemaker_processing",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
  ]
},
{
  "Sid" : "AllowRedshiftDataActions",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:CancelStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ]
}

```

```
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "AllowRedshiftGetClusterCredentials",
    "Effect" : "Allow",
    "Action" : [
        "redshift:GetClusterCredentials"
    ],
    "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
    ]
},
{
    "Sid" : "AllowListTagsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:ListTags"
    ],
    "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
    ]
},
{
    "Sid" : "AllowCloudformationListStackResources",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:ListStackResources"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
    "Sid" : "AllowS3ExpressObjectActions",
    "Effect" : "Allow",
    "Action" : [
        "s3express:CreateSession"
    ],
    "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
    ]
}
```

```

    "arn:aws:s3express:*:*:bucket/*aws-glue*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowS3ExpressCreateBucketActions",
  "Effect" : "Allow",
  "Action" : [
    "s3express:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3express:*:*:bucket/*SageMaker*",
    "arn:aws:s3express:*:*:bucket/*Sagemaker*",
    "arn:aws:s3express:*:*:bucket/*sagemaker*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowS3ExpressListBucketActions",
  "Effect" : "Allow",
  "Action" : [
    "s3express:ListAllMyDirectoryBuckets"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerGeospatialExecutionRole

설명: 이 정책은 SageMaker 지리공간 사용에 일반적으로 필요한 서비스에 대한 액세스를 제공합니다.

AmazonSageMakerGeospatialExecutionRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerGeospatialExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 11월 30일, 10:08 UTC
- 편집된 시간: 2023년 5월 10일, 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerGeospatialFullAccess

설명: 이 정책은 AWS Management Console 및 SDK를 통해 Amazon SageMaker Geospatial에 대한 전체 액세스를 허용하는 권한을 부여합니다.

AmazonSageMakerGeospatialFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerGeospatialFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2022년 11월 30일, 10:06 UTC
- 편집된 시간: 2022년 11월 30일, 10:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerGroundTruthExecution

설명: SageMaker GroundTruth 라벨링 작업을 실행하는 데 필요한 AWS 서비스에 대한 액세스를 제공합니다.

AmazonSageMakerGroundTruthExecution [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerGroundTruthExecution를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 9일, 19:30 UTC
- 편집된 시간: 2022년 4월 29일, 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerMechanicalTurkAccess

설명: 모든 워크팀을 대상으로 Amazon Augmented FlowDefinition AI 리소스를 생성할 수 있는 액세스를 제공합니다.

AmazonSageMakerMechanicalTurkAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerMechanicalTurkAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:19 UTC
- 편집된 시간: 2019년 12월 3일, 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerModelGovernanceUseAccess

설명: 이 AWS 관리형 정책은 모든 Amazon SageMaker Governance 기능을 사용하는 데 필요한 권한을 부여합니다. 또한 이 정책은 관련 서비스(예: S3, KMS)에 대한 선택적 액세스를 제공합니다.

AmazonSageMakerModelGovernanceUseAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerModelGovernanceUseAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 30일, 08:58 UTC
- 편집 시간: 2024년 6월 4일 21:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerModelRegistryFullAccess

설명: 이것은 Sagemaker의 모델 레지스트리에 대한 새로운 관리형 정책입니다. 이 정책은 사용자 역할에 연결하여 Sagemaker의 Model Registry 관련 기능에 액세스할 수 있는 독립형 정책입니다.

AmazonSageMakerModelRegistryFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerModelRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 13일, 05:20 UTC
- 편집 시간: 2024년 6월 6일 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerNotebooksServiceRolePolicy

설명: Amazon SageMaker 노트북의 서비스 연결 역할에 대한 관리형 정책

AmazonSageMakerNotebooksServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 18일, 20:27 UTC
- 편집 시간: 2024년 5월 22일 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

설명: Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 내에서 AWS APIGateway에서 사용하는 서비스 역할 정책입니다. Lambda 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy [관리형 정책](#)입니다. [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:06 UTC
- 편집된 시간: 2023년 8월 1일, 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 AWS CloudFormation 내에서 사용하는 서비스 역할 정책입니다. Lambda, APIGateway 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:06 UTC
- 편집된 시간: 2023년 8월 1일, 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

설명: Amazon 제품 포트폴리오의 프로비저닝된 AWS 제품 내에서 AWS ServiceCatalog Lambda가 사용하는 서비스 역할 정책입니다. SageMaker Secrets Manager 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:05 UTC
- 편집된 시간: 2023년 8월 1일, 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerPipelinesIntegrations

설명: 이 Amazon Managed Policy는 모델 구축 파이프라인의 콜백 단계 및 Lambda 단계와 SageMaker 함께 사용하는 데 일반적으로 필요한 권한을 부여합니다. Studio를 설정할 때 생성할 수 ExecutionRole 있는 AmazonSageMaker -에 추가됩니다. SageMaker 또한 파이프라인을 작성하거나 실행하는 데 사용되는 다른 모든 역할에 연결할 수도 있습니다.

AmazonSageMakerPipelinesIntegrations [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerPipelinesIntegrations를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 7월 30일, 16:35 UTC
- 편집된 시간: 2023년 2월 17일, 21:28 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerReadOnly

설명: AWS Management Console 및 SageMaker SDK를 통해 Amazon에 대한 읽기 전용 액세스를 제공합니다.

AmazonSageMakerReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 13:07 UTC
- 편집된 시간: 2021년 12월 1일, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

설명: Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 내에서 AWS APIGateway에서 사용하는 서비스 역할 정책입니다. 로그 및 기타를 비롯한 일련의 관련 서비스에 권한을 부여합니다. CloudWatch

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 3월 25일, 04:25 UTC
- 편집된 시간: 2022년 3월 25일, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 AWS CloudFormation 내에서 사용하는 서비스 역할 정책입니다. 등을 포함한 SageMaker 관련 서비스의 일부에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 3월 25일, 04:26 UTC
- 편집된 시간: 2022년 3월 25일, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 AWS CodeBuild 내에서 사용하는 서비스 역할 정책입니다. 등을 CodePipeline 포함한 CodeBuild 관련 서비스의 일부에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 3월 25일, 04:27 UTC
- 편집 시간: 2024년 6월 11일 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 AWS CodePipeline 내에서 사용하는 서비스 역할 정책입니다. 등을 CodePipeline 포함한 CodeBuild 관련 서비스의 일부에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:53 UTC
- 편집 시간: 2024년 6월 11일 18:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 내에서 AWS CloudWatch 이벤트에서 사용하는 서비스 역할 정책입니다. 등을 포함한 CodePipeline 관련 서비스의 일부에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:53 UTC
- 편집된 시간: 2022년 2월 22일, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

설명: Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 내에서 AWS Firehose에서 사용하는 서비스 역할 정책입니다. Firehose 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy [관리형 정책입니다.](#)
[다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:54 UTC
- 편집된 시간: 2022년 2월 22일, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

설명: Amazon 제품 SageMaker 포트폴리오의 AWS ServiceCatalog 프로비저닝된 제품 내에서 AWS Glue에서 사용하는 서비스 역할 정책입니다. Glue, S3 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:51 UTC
- 편집된 시간: 2022년 8월 26일, 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

설명: Amazon 제품 포트폴리오의 프로비저닝된 AWS 제품 내에서 AWS ServiceCatalog Lambda가 사용하는 서비스 역할 정책입니다. SageMaker ECR, S3 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 4일, 16:34 UTC
- 편집 시간: 2024년 6월 11일 18:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSecurityLakeAdministrator

설명: Amazon Security Lake 및 Security Lake를 관리하는 데 필요한 관련 서비스에 대한 전체 액세스 권한을 제공합니다.

AmazonSecurityLakeAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSecurityLakeAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 30일, 22:04 UTC
- 편집 시간: 2024년 2월 23일 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/apidestinatons.events.amazonaws.com/AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinatons.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource" : "arn:aws:iam:*:*:role/AmazonSecurityLake*",
    "Condition" : {

```

```

    "StringEquals" : {
      "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  },
  {
    "Sid" : "AllowRegisterS3LocationInLakeFormation",
    "Effect" : "Allow",
    "Action" : [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowIAMActionsByResource",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRolePolicies",
      "iam>DeleteRole"
    ],
    "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3ReadAccessToSecurityLakes",
    "Effect" : "Allow",
    "Action" : [
      "s3:Get*",
      "s3:List*"
    ]
  }
}

```

```

    ],
    "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid" : "S3ResourcelessReadOnly",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSecurityLakeMetastoreManager

설명: 클라우드워치, S3, Glue 및 SQS에 대한 액세스를 허용하는 Amazon SecurityLake 메타 스토어 관리자 램다에 대한 정책입니다.

AmazonSecurityLakeMetastoreManager [관리형AWS 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSecurityLakeMetastoreManager를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 작성 시간: 2024년 1월 23일 15:26 UTC
- 편집 시간: 2024년 4월 1일 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSecurityLakePermissionsBoundary

설명: Amazon Security Lake는 타사 사용자 지정 소스가 데이터 레이크에 데이터를 쓰고 타사 구독자가 데이터 레이크의 데이터를 사용할 수 있도록 IAM 역할을 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의합니다.

AmazonSecurityLakePermissionsBoundary [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSecurityLakePermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 29일, 14:11 UTC
- 편집 시간: 2024년 5월 14일 20:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSESEFullAccess

설명: 를 통해 Amazon SES에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AmazonSESEFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSESEFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESEFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSESReadOnlyAccess

설명: 를 통해 Amazon SES에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonSESReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSESReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 5월 14일 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
{
  "Sid" : "SESReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ses:Get*",
    "ses:List*",
    "ses:BatchGetMetricData"
  ],
  "Resource" : "*"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSESServiceRolePolicy

설명: SES가 SES 리소스를 대신하여 Amazon CloudWatch 기본 모니터링 지표를 게시할 수 있도록 합니다.

AmazonSESServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 5월 21일 16:02 UTC
- 편집 시간: 2024년 5월 21일 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSNSFullAccess

설명: 를 통해 Amazon SNS에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AmazonSNSFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSNSReadOnlyAccess

설명: 를 통해 Amazon SNS에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AmazonSNSReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSNSRole

설명: Amazon SNS 서비스 역할에 대한 기본 정책입니다.

AmazonSNSRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSQSFullAccess

설명: 를 통해 Amazon SQS에 대한 전체 액세스를 제공합니다. AWS Management Console

AmazonSQSFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSQSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSQSReadOnlyAccess

설명: 를 통해 Amazon SQS에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonSQSReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSQSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 5월 24일 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",

```

```
    "sqs:ListMessageMoveTasks",
    "sqs:ListQueueTags"
  ],
  "Resource" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMAutomationApproverAccess

설명: 자동화 실행을 확인하고 승인 대기 중인 자동화 팀에 승인 결정을 보낼 수 있는 액세스 권한을 제공합니다.

AmazonSSMAutomationApproverAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMAutomationApproverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 7일, 23:07 UTC
- 편집된 시간: 2017년 8월 7일, 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMAutomationRole

설명: EC2 자동화 서비스가 자동화 문서에 정의된 활동을 실행할 수 있는 권한을 제공합니다.

AmazonSSMAutomationRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMAutomationRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 5일, 22:09 UTC
- 편집된 시간: 2017년 7월 24일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMDirectoryServiceAccess

설명: 이 정책은 SSM 에이전트가 고객을 대신하여 Directory Service에 액세스하여 관리형 인스턴스에 도메인에 가입할 수 있도록 허용합니다.

AmazonSSMDirectoryServiceAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMDirectoryServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 3월 15일, 17:44 UTC
- 편집된 시간: 2019년 3월 15일, 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMFullAccess

설명: Amazon SSM에 대한 전체 액세스 권한을 제공합니다.

AmazonSSMFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 29일, 17:39 UTC
- 편집된 시간: 2019년 11월 20일, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMMaintenanceWindowRole

설명: EC2 유지 관리 기간에 사용할 서비스 역할

AmazonSSMMaintenanceWindowRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMMaintenanceWindowRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 1일, 15:57 UTC
- 편집된 시간: 2019년 7월 27일, 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

설명: 이 정책은 EC2 인스턴스에서 AWS Systems Manager 기능을 활성화합니다.

AmazonSSMManagedEC2InstanceDefaultPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMManagedEC2InstanceDefaultPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 30일, 20:54 UTC
- 편집된 시간: 2022년 8월 30일, 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMManagedInstanceCore

설명: AWS Systems Manager 서비스 핵심 기능을 활성화하기 위한 Amazon EC2 역할 정책입니다.

AmazonSSMManagedInstanceCore [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMManagedInstanceCore를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 3월 15일, 17:22 UTC
- 편집된 시간: 2019년 5월 23일, 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMPatchAssociation

설명: 패치 연결 작업을 위한 하위 인스턴스에 대한 액세스를 제공합니다.

AmazonSSMPatchAssociation [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMPatchAssociation를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 13일, 16:00 UTC
- 편집된 시간: 2020년 5월 13일, 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMReadOnlyAccess

설명: Amazon SSM에 대한 읽기 전용 액세스를 제공합니다.

AmazonSSMReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 29일, 17:44 UTC
- 편집된 시간: 2015년 5월 29일, 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSSMServiceRolePolicy

설명: Amazon SSM에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

AmazonSSMServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 13일, 19:20 UTC

- 편집된 시간: 2022년 9월 14일, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
```

```

    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SSM*",
    "arn:aws:lambda:*:*:function:*:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states:DescribeExecution",
    "states:StartExecution"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:SSM*",
    "arn:aws:states:*:*:execution:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:ListGroup",
    "resource-groups:ListGroupResources",
    "resource-groups:GetGroupQuery"
  ],
  "Resource" : [

```



```
    "*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:SelectResourceConfig"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "compute-optimizer:GetEC2InstanceRecommendations",
    "compute-optimizer:GetEnrollmentStatus"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "support:DescribeTrustedAdvisorChecks",
    "support:DescribeTrustedAdvisorCheckSummaries",
    "support:DescribeTrustedAdvisorCheckResult",
    "support:DescribeCases"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeComplianceByConfigRule",
    "config:DescribeComplianceByResource",
    "config:DescribeRemediationConfigurations",
    "config:DescribeConfigurationRecorders"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:DescribeAlarms",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "organizations:DescribeOrganization",
  "Resource" : "*"
},
{
```

```

    "Effect" : "Allow",
    "Action" : "cloudformation:ListStackSets",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStackInstances",
      "cloudformation:DescribeStackSetOperation",
      "cloudformation>DeleteStackSet"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudformation>DeleteStackInstances",
    "Resource" : [
      "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
      "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
      "arn:aws:cloudformation:*:*:type/resource/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:PutTargets"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "events:ManagedBy" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:RemoveTargets",
      "events>DeleteRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
    ]
  }

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonSumerianFullAccess

설명: Amazon Sumerian에 대한 전체 액세스 권한을 제공합니다.

AmazonSumerianFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSumerianFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 24일, 20:14 UTC
- 편집된 시간: 2018년 4월 24일, 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTextractFullAccess

설명: 모든 아마존 Textract API에 대한 액세스

AmazonTextractFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTextractFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 11월 28일, 19:07 UTC
- 편집된 시간: 2018년 11월 28일, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTextractServiceRole

설명: Texttract가 사용자 대신 AWS 서비스에 전화를 걸 수 있도록 허용합니다.

AmazonTextractServiceRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTextractServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 28일, 19:12 UTC
- 편집된 시간: 2018년 11월 28일, 19:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTimestreamConsoleFullAccess

설명: 를 사용하여 Amazon Timestream을 관리할 수 있는 전체 액세스 권한을 제공합니다. AWS Management Console참고로 이 정책은 특정 KMS 작업 및 저장된 쿼리를 관리하는 작업에 대한 권한도 부여합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

AmazonTimestreamConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2022년 2월 1일, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTimestreamFullAccess

설명: Amazon Timestream에 대한 전체 액세스 권한을 제공합니다. 참고로 이 정책은 특정 KMS 작업 액세스 권한도 부여합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

AmazonTimestreamFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2021년 11월 26일, 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTimestreamInfluxDBFullAccess

설명: Amazon Timestream InfluxDB 인스턴스를 생성, 업데이트, 삭제 및 나열하고 파라미터 그룹을 생성 및 나열할 수 있는 전체 관리 액세스 권한을 제공합니다. 필요한 추가 권한은 설명서를 참조하십시오.

AmazonTimestreamInfluxDBFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamInfluxDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 3월 14일 22:53 UTC
- 편집 시간: 2024년 3월 14일 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTimestreamInfluxDBServiceRolePolicy

설명: Amazon Timestream InfluxDB 인스턴스를 생성, 업데이트, 삭제 및 나열하고 파라미터 그룹을 생성 및 나열할 수 있는 전체 관리 액세스 권한을 제공합니다. 필요한 추가 권한은 설명서를 참조하십시오.

AmazonTimestreamInfluxDBServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 3월 14일 18:53 UTC
- 편집 시간: 2024년 3월 14일 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTimestreamReadOnlyAccess

설명: Amazon Timestream에 대한 읽기 전용 액세스를 제공합니다. 정책은 실행 중인 모든 쿼리를 취소할 수 있는 권한도 제공합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

AmazonTimestreamReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집 시간: 2024년 6월 5일 19:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTranscribeFullAccess

설명: Amazon Transcribe 작업에 대한 전체 액세스 권한을 제공합니다.

AmazonTranscribeFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTranscribeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 4일, 16:06 UTC
- 편집된 시간: 2018년 4월 4일, 16:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*transcribe*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonTranscribeReadOnlyAccess

설명: Amazon Transcribe의 읽기 전용 작업에 대한 액세스를 제공합니다.

AmazonTranscribeReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTranscribeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 4일, 16:05 UTC
- 편집된 시간: 2018년 4월 4일, 16:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

설명: 네트워크 인터페이스를 생성하여 계정 간 리소스에 연결할 수 있는 액세스 권한을 제공합니다.

AmazonVPCCrossAccountNetworkInterfaceOperations [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCCrossAccountNetworkInterfaceOperations를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 7월 18일, 20:47 UTC
- 편집된 시간: 2023년 9월 25일, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCFullAccess

설명: 를 통해 Amazon VPC에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonVPCFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 2월 8일 16:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

설명: Network Insights 액세스 범위 및 Network Insights 액세스 범위 분석에서 AWS 리소스를 설명하고, Network Access Analyzer를 실행하고, 태그를 생성 또는 삭제할 수 있는 권한을 제공합니다.

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCNetworkAccessAnalyzerFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 15일, 22:56 UTC
- 편집 시간: 2024년 5월 15일 21:40 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

설명: 네트워크 인사이트 경로 및 네트워크 인사이트 분석에서 AWS 리소스를 설명하고, Reachability Analyzer를 실행하고, 태그를 생성 또는 삭제할 수 있는 권한을 제공합니다.

AmazonVPCReachabilityAnalyzerFullAccessPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCReachabilityAnalyzerFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 14일, 20:12 UTC
- 편집 시간: 2024년 5월 15일 20:47 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerFullAccessPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2>DeleteNetworkInsightsAnalysis",
        "ec2>DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```

    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAnalysis"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2TagsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-path/*",
    "arn:*:ec2:*:*:network-insights-analysis/*"
  ]
},
{
  "Sid" : "ElasticloadbalancingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ]
}

```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GlobalacceleratorPermissions",
    "Effect" : "Allow",
    "Action" : [
      "globalaccelerator:ListAccelerators",
      "globalaccelerator:ListCustomRoutingAccelerators",
      "globalaccelerator:ListCustomRoutingEndpointGroups",
      "globalaccelerator:ListCustomRoutingListeners",
      "globalaccelerator:ListCustomRoutingPortMappings",
      "globalaccelerator:ListEndpointGroups",
      "globalaccelerator:ListListeners"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "NetworkFirewallPermissions",
    "Effect" : "Allow",
    "Action" : [
      "network-firewall:DescribeFirewall",
      "network-firewall:DescribeFirewallPolicy",
      "network-firewall:DescribeResourcePolicy",
      "network-firewall:DescribeRuleGroup",
      "network-firewall:ListFirewallPolicies",
      "network-firewall:ListFirewalls",
      "network-firewall:ListRuleGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TiroPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tiros:CreateQuery",
      "tiros:ExtendQuery",
      "tiros:GetQueryAnswer",
      "tiros:GetQueryExplanation",
      "tiros:GetQueryExtensionAccounts"
    ],
    "Resource" : "*"
  }
]
```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

설명: 이 정책은 IAM RoleForReachabilityAnalyzerCrossAccountResourceAccess 역할에 연결되어 있습니다. 이 역할은 관리 계정을 통해 Reachability Analyzer에 대한 신뢰할 수 있는 액세스를 활성화할 때 조직의 멤버 계정에 배포됩니다. Reachability Analyzer 콘솔을 사용하여 조직 전체의 리소스를 볼 수 있는 권한을 제공합니다.

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCReachabilityAnalyzerPathComponentReadPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 1일, 20:38 UTC
- 편집된 시간: 2023년 5월 1일, 20:38 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonVPCReadOnlyAccess

설명: 를 통해 Amazon VPC에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AmazonVPCReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 2월 8일 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkDocsFullAccess

설명: 를 WorkDocs 통해 Amazon에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AmazonWorkDocsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkDocsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 16일, 23:05 UTC
- 편집된 시간: 2020년 4월 16일, 23:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkDocsReadOnlyAccess

설명: 를 WorkDocs 통해 Amazon에 대한 읽기 전용 액세스 권한을 제공합니다. AWS Management Console

AmazonWorkDocsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkDocsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 8일, 23:49 UTC
- 편집된 시간: 2020년 1월 8일, 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "workdocs:Describe*",
      "ds:DescribeDirectories",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkMailEventsServiceRolePolicy

설명: Amazon WorkMail Events에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다.

AmazonWorkMailEventsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 4월 16일, 16:52 UTC
- 편집된 시간: 2019년 4월 16일, 16:52 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkMailFullAccess

설명: Directory Service, SES WorkMail, EC2에 대한 전체 액세스 권한과 KMS 메타데이터에 대한 읽기 권한을 제공합니다.

AmazonWorkMailFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkMailFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 12월 21일, 14:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkMailMessageFlowFullAccess

설명: WorkMail 메시지 흐름 API에 대한 전체 권한

AmazonWorkMailMessageFlowFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkMailMessageFlowFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 2월 11일, 11:08 UTC
- 편집된 시간: 2021년 2월 11일, 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkMailMessageFlowReadOnlyAccess

설명: GetRawMessageContent API의 WorkMail 메시지에 대한 읽기 전용 액세스

AmazonWorkMailMessageFlowReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkMailMessageFlowReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 28일, 12:40 UTC
- 편집된 시간: 2021년 1월 28일, 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkMailReadOnlyAccess

설명: WorkMail 및 SES에 대한 읽기 전용 액세스를 제공합니다.

AmazonWorkMailReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkMailReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 7월 25일, 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesAdmin

설명: AWS SDK 및 CLI를 통해 Amazon WorkSpaces 관리 작업에 액세스할 수 있습니다.

AmazonWorkSpacesAdmin [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesAdmin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 9월 22일, 22:21 UTC

- 편집된 시간: 2023년 8월 3일, 23:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesApplicationManagerAdminAccess

설명: Amazon WorkSpaces Application Manager에서 애플리케이션을 패키징하기 위한 관리자 액세스 권한을 제공합니다.

AmazonWorkSpacesApplicationManagerAdminAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesApplicationManagerAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 14:03 UTC
- 편집된 시간: 2015년 4월 9일, 14:03 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonWorkSpacesApplicationManagerAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkspacesPCAAccess

설명: 이 관리형 정책은 AWS 인증서 기반 인증을 위해 사용자의 Certificate Manager 사설 CA 리소스에 AWS 계정 대한 전체 관리 액세스를 제공합니다.

AmazonWorkspacesPCAAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkspacesPCAAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 11월 8일, 00:25 UTC
- 편집된 시간: 2022년 11월 8일, 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesSelfServiceAccess

설명: Workspace 셀프 서비스 작업을 수행할 수 있도록 Amazon WorkSpaces 백엔드 서비스에 대한 액세스를 제공합니다.

AmazonWorkSpacesSelfServiceAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesSelfServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 19:22 UTC
- 편집된 시간: 2019년 6월 27일, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
    },
  ],
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesServiceAccess

설명: Workspace를 시작하기 위한 AWS WorkSpaces 서비스에 대한 고객 계정 액세스를 제공합니다.

AmazonWorkSpacesServiceAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 19:19 UTC
- 편집된 시간: 2020년 3월 18일, 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesWebReadOnly

설명: AWS Management Console, SDK 및 CLI를 통해 Amazon WorkSpaces Web 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.

AmazonWorkSpacesWebReadOnly [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesWebReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 30일, 14:20 UTC

- 편집된 시간: 2022년 11월 2일, 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonWorkSpacesWebServiceRolePolicy

설명: Amazon WorkSpaces Web에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다.

AmazonWorkSpacesWebServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 30일, 13:15 UTC
- 편집된 시간: 2022년 12월 15일, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonZocaloFullAccess

설명: Amazon Zocalo에 대한 전체 액세스 권한을 제공합니다.

AmazonZocaloFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonZocaloFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmazonZocaloReadOnlyAccess

설명: Amazon Zocalo에 대한 읽기 전용 액세스 권한을 제공합니다.

AmazonZocaloReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonZocaloReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

```
    "ds:DescribeDirectories",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AmplifyBackendDeployFullAccess

설명: 개발 키트 (CDK) 를 통해 Amplify 백엔드 리소스 (Amazon AWS AppSync Cognito, Amazon S3 및 기타 관련 서비스) 를 배포할 수 있는 Amplify 전체 액세스 권한을 제공합니다. AWS 클라우드 AWS

AmplifyBackendDeployFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AmplifyBackendDeployFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 6일, 21:32 UTC
- 편집 시간: 2024년 5월 31일 15:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

APIGatewayServiceRolePolicy

설명: API Gateway가 고객을 대신하여 관련 AWS 리소스를 관리할 수 있도록 허용합니다.

APIGatewayServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 17:23 UTC
- 편집된 시간: 2021년 7월 12일, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AppIntegrationsServiceLinkedRolePolicy

설명: 사용자를 대신하여 AppFlow 리소스를 관리하고 CloudWatch 지표 데이터를 게시할 수 있습니다.
AppIntegrations

AppIntegrationsServiceLinkedRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 30일, 19:42 UTC
- 편집된 시간: 2022년 9월 30일, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ApplicationAutoScalingForAmazonAppStreamAccess

설명: Amazon용 애플리케이션 자동 확장을 활성화하는 정책 AppStream

ApplicationAutoScalingForAmazonAppStreamAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ApplicationAutoScalingForAmazonAppStreamAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 2월 6일, 21:39 UTC
- 편집된 시간: 2017년 2월 6일, 21:39 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

설명: Application Discovery Service 연속 내보내기 기능에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 사용할 수 있도록 합니다.

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 9일, 20:22 UTC
- 편집된 시간: 2018년 8월 13일, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AppRunnerNetworkingServiceRolePolicy

설명: AWS AppRunner 네트워킹이 사용자를 대신하여 관련 AWS 리소스를 관리할 수 있도록 합니다.

AppRunnerNetworkingServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 1월 12일, 21:02 UTC
- 편집된 시간: 2022년 1월 12일, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AppRunnerServiceRolePolicy

설명: 사용자 대신 관련 AWS 리소스를 관리할 수 있습니다. AWS AppRunner

AppRunnerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 14일, 19:15 UTC
- 편집된 시간: 2021년 5월 14일, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingConsoleFullAccess

설명: 를 통해 Auto Scaling에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AutoScalingConsoleFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:43 UTC
- 편집된 시간: 2018년 2월 6일, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingConsoleReadOnlyAccess

설명: 를 통해 Auto Scaling에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console AutoScalingConsoleReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:48 UTC
- 편집된 시간: 2017년 1월 12일, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingFullAccess

설명: Auto Scaling에 대한 전체 액세스 권한을 제공합니다.

AutoScalingFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:31 UTC
- 편집된 시간: 2018년 2월 6일, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingNotificationAccessRole

설명: AutoScaling 알림 액세스 서비스 역할의 기본 정책입니다.

AutoScalingNotificationAccessRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingNotificationAccessRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingReadOnlyAccess

설명: Auto Scaling에 대한 읽기 전용 액세스를 제공합니다.

AutoScalingReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 `AutoScalingReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:39 UTC
- 편집된 시간: 2017년 1월 12일, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AutoScalingServiceRolePolicy

설명: Auto Scaling에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다.

AutoScalingServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 1월 8일, 23:10 UTC
- 편집 시간: 2024년 2월 29일 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWS_ConfigRole

설명: AWS Config 서비스 역할에 대한 기본 정책입니다. AWS Config가 리소스 변경 사항을 추적하는데 필요한 권한을 제공합니다. AWS

AWS_ConfigRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWS_ConfigRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2020년 9월 15일, 20:30 UTC
- 편집 시간: 2024년 2월 22일 21:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

정책 버전

정책 버전: v30(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]

```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAccountActivityAccess

설명: 사용자가 계정 활동 페이지에 액세스할 수 있습니다.

AWSAccountActivityAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAccountActivityAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2023년 3월 7일, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAccountManagementFullAccess

설명: AWS 계정 관리에 대한 전체 액세스 권한을 제공합니다.

AWSAccountManagementFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAccountManagementFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 30일, 23:20 UTC
- 편집된 시간: 2021년 9월 30일, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAccountManagementReadOnlyAccess

설명: AWS 계정 관리에 대한 읽기 전용 액세스를 제공합니다.

AWSAccountManagementReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSAccountManagementReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 30일, 23:29 UTC
- 편집된 시간: 2021년 9월 30일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAccountUsageReportAccess

설명: 사용자가 계정 사용 보고서 페이지에 액세스할 수 있습니다.

AWSAccountUsageReportAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSAccountUsageReportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "aws-portal:ViewUsage"
  ],
  "Resource" : "*"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAgentlessDiscoveryService

설명: 디스커버리 에이전트리스 커넥터가 AWS Application Discovery Service에 등록할 수 있도록 액세스를 제공합니다.

AWSAgentlessDiscoveryService [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAgentlessDiscoveryService를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 8월 2일, 01:35 UTC
- 편집된 시간: 2020년 2월 24일, 23:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppFabricFullAccess

설명: AWS AppFabric 서비스에 대한 전체 액세스 권한과 S3, Kinesis, KMS와 같은 종속 서비스에 대한 읽기 전용 액세스를 제공합니다.

AWSAppFabricFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppFabricFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 19:51 UTC
- 편집된 시간: 2023년 6월 27일, 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
]
```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppFabricReadOnlyAccess

설명: 에 대한 읽기 전용 액세스 권한을 제공합니다. AWS AppFabric

AWSAppFabricReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSAppFabricReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 19:52 UTC
- 편집된 시간: 2023년 6월 27일, 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppFabricServiceRolePolicy

설명: 사용자를 대신하여 AWS 리소스에 대한 AppFabric 액세스를 제공합니다.

AWSAppFabricServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 26일, 21:07 UTC
- 편집된 시간: 2023년 6월 26일, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

설명: Application Auto Scaling에 AppStream 및 CloudWatch 에 대한 액세스 권한을 부여하는 정책.

AWSApplicationAutoscalingAppStreamFleetPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 19:04 UTC
- 편집된 시간: 2017년 10월 20일, 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```


자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingCassandraTablePolicy

설명: Application Auto Scaling에 카산드라에 액세스할 수 있는 권한을 부여하는 정책. CloudWatch

AWSApplicationAutoscalingCassandraTablePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 3월 18일, 22:49 UTC
- 편집된 시간: 2020년 3월 18일, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

설명: Comprehend 및 에 액세스할 수 있는 권한을 Application Auto Scaling에 부여하는 정책
CloudWatch

AWSApplicationAutoscalingComprehendEndpointPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 11월 14일, 18:39 UTC
- 편집된 시간: 2019년 11월 14일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSApplicationAutoscalingComprehendEndpointPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoScalingCustomResourcePolicy

설명: Application Auto Scaling에 API Gateway에 액세스하고 CloudWatch 사용자 지정 리소스 크기 조정을 위한 권한을 부여하는 정책

AWSApplicationAutoScalingCustomResourcePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 4일, 23:22 UTC
- 편집된 시간: 2018년 6월 4일, 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```

    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

설명: 애플리케이션 Auto Scaling에 DynamoDB 및 에 액세스할 수 있는 권한을 부여하는 정책.
CloudWatch

AWSApplicationAutoscalingDynamoDBTablePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 21:34 UTC
- 편집된 시간: 2017년 10월 20일, 21:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

설명: Application Auto Scaling에 EC2 스팟 플릿 및 에 액세스할 수 있는 권한을 부여하는 정책
CloudWatch

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 25일, 18:23 UTC
- 편집된 시간: 2017년 10월 25일, 18:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingECSServicePolicy

설명: Application Auto Scaling에 EC2 컨테이너 서비스에 액세스할 수 있는 권한을 부여하는 정책 및 CloudWatch

AWSApplicationAutoscalingECSServicePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 25일, 23:53 UTC
- 편집된 시간: 2017년 10월 25일, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```



```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeServices",
      "ecs:UpdateService",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

설명: ElastiCache Amazon과 Amazon에 액세스할 수 있는 권한을 Application Auto Scaling에 부여하는 정책입니다. CloudWatch

AWSApplicationAutoscalingElastiCacheRGPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 17일, 23:41 UTC

- 편집된 시간: 2021년 8월 17일, 23:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

설명: Elastic Map Reduce 및 CloudWatch 에 액세스할 수 있는 권한을 Application Auto Scaling에 부여하는 정책

AWSApplicationAutoscalingEMRInstanceGroupPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 26일, 00:57 UTC
- 편집된 시간: 2017년 10월 26일, 00:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingKafkaClusterPolicy

설명: Application Auto Scaling에 Apache Managed Kafka용 관리형 스트리밍에 액세스할 수 있는 권한을 부여하는 정책 및 CloudWatch

AWSApplicationAutoscalingKafkaClusterPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2020년 8월 24일, 18:36 UTC
- 편집된 시간: 2020년 8월 24일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

설명: 애플리케이션 Auto Scaling에 Lambda 및 에 액세스할 수 있는 권한을 부여하는 정책.
CloudWatch

AWSApplicationAutoscalingLambdaConcurrencyPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 21일, 20:04 UTC
- 편집된 시간: 2019년 10월 21일, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",

```

```

    "cloudwatch:DescribeAlarms",
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

설명: Amazon CloudWatch Neptune과 Amazon에 액세스할 수 있는 권한을 Application Auto Scaling에 부여하는 정책입니다.

AWSApplicationAutoscalingNeptuneClusterPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 2일, 21:14 UTC
- 편집된 시간: 2021년 9월 2일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingRDSClusterPolicy

설명: Application Auto Scaling에 RDS 및 에 액세스할 수 있는 권한을 부여하는 정책 CloudWatch

AWSApplicationAutoscalingRDSClusterPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 17일, 17:46 UTC
- 편집된 시간: 2018년 8월 7일, 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

설명: Application Auto Scaling에 SageMaker 및 CloudWatch 에 대한 액세스 권한을 부여하는 정책.

AWSApplicationAutoscalingSageMakerEndpointPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 2월 6일, 19:58 UTC
- 편집된 시간: 2023년 11월 13일, 18:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationDiscoveryAgentAccess

설명: 검색 에이전트가 AWS Application Discovery Service에 등록할 수 있는 액세스 권한을 제공합니다.

AWSApplicationDiscoveryAgentAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationDiscoveryAgentAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 5월 11일, 21:38 UTC
- 편집된 시간: 2020년 2월 24일, 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

설명: Application Discovery Service 에이전트 없는 수집기가 Application Discovery Service와 자동 업데이트, 등록 및 통신할 수 있도록 합니다.

AWSApplicationDiscoveryAgentlessCollectorAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationDiscoveryAgentlessCollectorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 21:00 UTC
- 편집된 시간: 2022년 8월 16일, 21:00 UTC

- ARN: arn:aws:iam::aws:policy/
AWSApplicationDiscoveryAgentlessCollectorAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationDiscoveryServiceFullAccess

설명: AWS Application Discovery Service에서 유지 관리하는 구성 항목을 보고 태그를 지정할 수 있는 전체 액세스 권한을 제공합니다.

AWSApplicationDiscoveryServiceFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationDiscoveryServiceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 5월 11일, 21:30 UTC
- 편집된 시간: 2019년 6월 19일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationAgentInstallationPolicy

설명: 이 정책은 MGN (AWS 응용 프로그램 마이그레이션 서비스) 과 함께 외부 서버를 마이그레이션 하는 데 사용되는 AWS 복제 에이전트를 설치할 수 있도록 AWS합니다. AWS 복제 에이전트를 설치할 때 자격 증명을 제공하는 IAM 사용자 또는 역할에 이 정책을 연결하십시오.

AWSApplicationMigrationAgentInstallationPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationAgentInstallationPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 6월 19일, 07:51 UTC
- 편집된 시간: 2022년 9월 20일, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationAgentPolicy

설명: 이 정책은 MGN (AWS 응용 프로그램 마이그레이션 서비스) 과 함께 외부 서버를 마이그레이션 하는 데 사용되는 AWS 복제 에이전트의 설치 및 사용을 허용합니다. AWS 복제 에이전트를 설치 할 때 자격 증명을 제공하는 IAM 사용자 또는 역할에 이 정책을 연결하십시오.

AWSApplicationMigrationAgentPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationAgentPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 4월 7일, 07:00 UTC
- 편집된 시간: 2022년 9월 20일, 11:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationAgentPolicy_v2

설명: 이 정책은 MGN (AWS 응용 프로그램 마이그레이션 서비스) 과 함께 외부 서버를 마이그레이션 하는 데 사용되는 AWS 복제 에이전트를 사용할 수 있도록 AWS 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSApplicationMigrationAgentPolicy_v2 [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationAgentPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 6월 6일, 14:14 UTC
- 편집된 시간: 2022년 6월 6일, 14:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationConversionServerPolicy

설명: 이 정책은 애플리케이션 마이그레이션 서비스에서 시작하는 EC2 인스턴스인 애플리케이션 마이그레이션 서비스 (MGN) 전환 서버가 MGN 서비스와 통신할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery에 의해 (EC2 Instance Profile로) MGN Conversion Servers에 연결되며, 필요할 때 MGN에 의해 자동으로 시작 및 종료됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다. MGN Conversion Servers는 사용자가 MGN 콘솔, CLI 또는 API를 사용하여 테스트 또는 컷오버 인스턴스를 시작하도록 선택할 때 Application Migration Service에서 사용됩니다.

AWSApplicationMigrationConversionServerPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationConversionServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 06:48 UTC
- 편집된 시간: 2021년 4월 7일, 06:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```

{
  "Effect" : "Allow",
  "Action" : [
    "mgn:SendClientMetricsForMgn",
    "mgn:SendClientLogsForMgn",
    "mgn:GetChannelCommandsForMgn",
    "mgn:SendChannelCommandResultForMgn"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationEC2Access

설명: 이 정책은 애플리케이션 마이그레이션 서비스 (MGN) 를 사용하여 마이그레이션된 서버를 EC2 인스턴스로 시작하는 데 필요한 Amazon EC2 작업을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWSApplicationMigrationEC2Access [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationEC2Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 07:05 UTC
- 편집된 시간: 2023년 2월 6일, 16:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationFullAccess

설명: 이 정책은 AWS 애플리케이션 마이그레이션 서비스 (MGN) 의 모든 퍼블릭 API에 대한 권한과 KMS 키 정보를 읽을 수 있는 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWSApplicationMigrationFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 06:56 UTC
- 편집 시간: 2024년 5월 19일 08:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationMGHAccess

설명: 이 정책을 통해 AWS 응용 프로그램 마이그레이션 서비스 (MGN) 는 MGN을 사용하여 마이그레이션되는 서버의 진행 상황에 대한 메타데이터를 MGH (Migration AWS Hub) 로 전송할 수 있습니다.

MGN은 이 정책이 연결된 IAM 역할을 자동으로 생성하고 이 역할을 맡습니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSApplicationMigrationMGHAccess관리형 [AWS 정책입니다](#).

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationMGHAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 07:10 UTC
- 편집된 시간: 2021년 4월 7일, 07:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationReadOnlyAccess

설명: 이 정책은 응용 프로그램 마이그레이션 서비스 (MGN) 의 모든 읽기 전용 공용 API와 MGN 콘솔을 완전히 읽기 전용으로 사용하는 데 필요한 다른 AWS 서비스의 일부 읽기 전용 API에 대한 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWSApplicationMigrationReadOnlyAccess관리형 [AWS 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 07:15 UTC
- 편집된 시간: 2023년 3월 20일, 08:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationReplicationServerPolicy

설명: 이 정책은 애플리케이션 마이그레이션 서비스에서 시작하는 EC2 인스턴스인 애플리케이션 마이그레이션 서비스 (MGN) 복제 서버가 MGN 서비스와 통신하고 사용자의 EBS 스냅샷을 생성할 수 있도록 허용합니다. AWS 계정이 정책이 있는 IAM 역할은 Application Migration Service에 의해 (EC2 Instance Profile로) MGN Replication Servers에 연결되며, 필요에 따라 MGN에 의해 자동으로 시작 및 종료됩니다. MGN 복제 서버는 MGN을 사용하여 관리되는 마이그레이션 프로세스의 일환으로 외부 서버에서 외부 서버로의 AWS데이터 복제를 용이하게 하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSApplicationMigrationReplicationServerPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationReplicationServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 07:21 UTC
- 편집된 시간: 2021년 4월 7일, 07:21 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationServiceEc2InstancePolicy

설명: 이 정책은 AWS 애플리케이션 마이그레이션 서비스 (AWS MGN) 에서 EC2에서 실행되는 원본 서버 (지역 간 또는 교차 AZ) 를 마이그레이션하는 데 사용하는 AWS 복제 에이전트의 설치 및 사용을 허용합니다. 이 정책이 있는 IAM 역할은 EC2 Instances에 (EC2 Instance Profile로) 연결되어야 합니다.

AWSApplicationMigrationServiceEc2InstancePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationServiceEc2InstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 22일, 13:19 UTC
- 편집 시간: 2024년 1월 3일 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationServiceRolePolicy

설명: AWS 애플리케이션 마이그레이션 서비스가 사용자를 대신하여 AWS 리소스를 생성하고 관리할 수 있도록 합니다.

AWSApplicationMigrationServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 7일, 06:43 UTC
- 편집된 시간: 2023년 6월 20일, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
```

```
    "ec2:DescribeVolumes",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount"
  ],
  "Resource" : "arn:aws:organizations::*:account/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateLaunchTemplateVersion",
  "ec2:ModifyLaunchTemplate",
  "ec2>DeleteLaunchTemplate",
  "ec2>DeleteLaunchTemplateVersions"
],
"Resource" : "arn:aws:ec2:*:*:launch-template/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:RevokeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:AuthorizeSecurityGroupEgress"
],
"Resource" : "arn:aws:ec2:*:*:security-group/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
```

```
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
```

```

    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
    "arn:aws:iam:*:*:role/service-role/AWSApplicationMigrationConversionServerRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate",
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    }
  }
}
]

```


}

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationSSMAccess

설명: 이 정책은 애플리케이션 마이그레이션 서비스 (MGN) 를 사용하여 사용자 지정 마이그레이션 후 명령 SSM 문서를 실행하는 데 필요한 Amazon SSM 작업에 대한 액세스를 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWSApplicationMigrationSSMAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationSSMAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 09:29 UTC
- 편집된 시간: 2023년 3월 20일, 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSApplicationMigrationVCenterClientPolicy

설명: 이 정책은 MGN (AWS 응용 프로그램 마이그레이션 서비스) 과 함께 외부 서버를 마이그레이션 하는 데 사용되는 AWS vCenter Client의 설치 및 사용을 허용합니다. AWS vCenter Client를 설치할 때 자격 증명을 제공하는 IAM 사용자 또는 역할에 이 정책을 연결하십시오. AWS

AWSApplicationMigrationVCenterClientPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationVCenterClientPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 8일, 12:53 UTC
- 편집된 시간: 2021년 11월 8일, 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshEnvoyAccess

설명: 가상 노드 구성에 액세스하기 위한 App Mesh Envoy 정책입니다.

AWSAppMeshEnvoyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshEnvoyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 3일, 21:29 UTC

- 편집된 시간: 2019년 7월 3일, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshFullAccess

설명: AWS App Mesh API 및 관리 콘솔에 대한 전체 액세스 권한을 제공합니다.

AWSAppMeshFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAppMeshFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 16일, 17:50 UTC
- 편집된 시간: 2021년 1월 7일, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshPreviewEnvoyAccess

설명: 가상 노드 구성에 액세스하기 위한 App Mesh Preview Envoy 정책입니다.

AWSAppMeshPreviewEnvoyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshPreviewEnvoyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 8월 5일, 23:32 UTC
- 편집된 시간: 2019년 8월 5일, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ]
    }
  ]
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshPreviewServiceRolePolicy

설명: AWS App Mesh에서 사용하거나 관리하는 리소스에 대한 액세스 AWS 서비스 및 리소스를 활성화합니다.

AWSAppMeshPreviewServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 19일, 19:07 UTC
- 편집된 시간: 2019년 8월 21일, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshReadOnly

설명: AWS App Mesh API 및 관리 콘솔에 대한 읽기 전용 액세스를 제공합니다.

AWSAppMeshReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 16일, 17:51 UTC
- 편집된 시간: 2021년 1월 7일, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppMeshServiceRolePolicy

설명: 리소스를 사용하거나 관리하는 리소스에 AWS 서비스 액세스할 수 있도록 합니다. AWS AppMesh

AWSAppMeshServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 3일, 18:30 UTC
- 편집된 시간: 2023년 10월 10일, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppRunnerFullAccess

설명: 모든 App Runner 작업에 권한을 부여합니다.

AWSAppRunnerFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppRunnerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 1월 11일, 04:02 UTC
- 편집된 시간: 2022년 1월 11일, 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppRunnerReadOnlyAccess

설명: App Runner 리소스의 세부 정보를 나열하고 볼 수 있는 권한을 부여합니다.

AWSAppRunnerReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAppRunnerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 24일, 21:24 UTC
- 편집된 시간: 2022년 2월 24일, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppRunnerServicePolicyForECRAccess

설명: 고객 계정의 Amazon ECR 리소스에 읽기 권한을 부여하는 AWS App Runner 서비스 정책입니다. App Runner 서비스를 생성하거나 업데이트할 때 App Runner에 전달되는 역할에 사용하세요.

AWSAppRunnerServicePolicyForECRAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppRunnerServicePolicyForECRAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 5월 14일, 19:17 UTC
- 편집된 시간: 2021년 5월 14일, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
      "ecr:DescribeImages",
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppSyncAdministrator

설명: AppSync 서비스에 대한 관리 액세스를 제공하지만 콘솔을 통해 액세스하기에는 충분하지 않습니다.

AWSAppSyncAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:20 UTC
- 편집된 시간: 2019년 11월 4일, 19:23 UTC

- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppSyncInvokeFullAccess

설명: 콘솔을 통하거나 독립적으로 AppSync 서비스에 대한 전체 호출 액세스를 제공합니다.

AWSAppSyncInvokeFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncInvokeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:21 UTC
- 편집된 시간: 2018년 3월 20일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppSyncPushToCloudWatchLogs

설명: 로그를 사용자 CloudWatch 계정으로 AppSync 푸시할 수 있습니다.

AWSAppSyncPushToCloudWatchLogs [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAppSyncPushToCloudWatchLogs`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 4월 9일, 19:38 UTC
- 편집된 시간: 2018년 4월 9일, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppSyncSchemaAuthor

설명: 스키마를 생성, 업데이트 및 쿼리할 수 있는 액세스 권한을 제공합니다.

AWSAppSyncSchemaAuthor [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncSchemaAuthor를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:21 UTC
- 편집된 시간: 2023년 2월 1일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAppSyncServiceRolePolicy

설명: 에서 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있습니다. AppSync

AWSAppSyncServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 1월 21일, 19:56 UTC
- 편집된 시간: 2020년 1월 21일, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSArtifactAccountSync

설명: AWS Organizations의 작업에 대한 Artifact 읽기 전용 액세스를 허용합니다. AWS

AWSArtifactAccountSync [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSArtifactAccountSync를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 4월 10일, 23:04 UTC
- 편집된 시간: 2018년 4월 10일, 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSArtifactReportsReadOnlyAccess

설명: AWS Artifact 서비스 보고서에 대한 읽기 전용 액세스를 제공합니다.

AWSArtifactReportsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSArtifactReportsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 1월 2일 22:42 UTC
- 편집 시간: 2024년 1월 2일 22:42 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSArtifactServiceRolePolicy

설명: AWS Artifact가 Organizations 서비스를 통해 AWS 조직에 대한 정보를 수집할 수 있도록 합니다.

AWSArtifactServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 8월 21일, 20:27 UTC
- 편집된 시간: 2023년 8월 21일, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",

```

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAuditManagerAdministratorAccess

설명: AWS Audit Manager를 활성화 또는 비활성화하고, 설정을 업데이트하고, 평가, 제어 및 프레임워크를 관리할 수 있는 관리 액세스 권한을 제공합니다.

AWSAuditManagerAdministratorAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAuditManagerAdministratorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 11일, 20:02 UTC
- 편집 시간: 2024년 5월 15일 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAuditManagerServiceRolePolicy

설명: AWS Audit Manager에서 사용하거나 관리하는 리소스 AWS 서비스 및 리소스에 액세스할 수 있습니다.

AWSAuditManagerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 8일, 15:12 UTC
- 편집 시간: 2024년 6월 10일 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

설명: 조정 계획의 AWS Auto Scaling 그룹에 대해 주기적으로 용량을 예측하고 스케줄링된 조정 작업을 생성할 수 있는 권한을 Auto Scaling에 부여하는 정책

AWSAutoScalingPlansEC2AutoScalingPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 23일, 22:46 UTC
- 편집된 시간: 2018년 8월 23일, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupAuditAccess

설명: 이 정책은 사용자에게 AWS Backup 리소스 및 활동에 대한 기대치를 정의하는 제어 및 프레임워크를 만들고 정의된 제어 및 프레임워크에 대해 AWS Backup 리소스 및 활동을 감사할 수 있는 권한을 부여합니다. 이 정책은 AWS Config 및 유사 서비스에 감사를 수행할 사용자 기대치를 설명하는 권한을 부여합니다. 또한 이 정책은 S3 및 유사한 서비스에 감사 보고서를 전송할 수 있는 권한을 부여하고 사용자가 감사 보고서를 검색하고 열람할 수 있도록 합니다.

AWSBackupAuditAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupAuditAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 24일, 01:02 UTC
- 편집된 시간: 2023년 4월 10일, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupDataTransferAccess

설명: 이 정책은 AWS Backint 에이전트가 Backup Storage 플레인을 사용하여 AWS 백업 데이터 전송을 완료할 수 있도록 합니다. 이 역할을 Backint 에이전트와 함께 SAP HANA를 실행하는 Amazon EC2 Instances가 맡은 역할에 연결하세요.

AWSBackupDataTransferAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupDataTransferAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 22:48 UTC
- 편집된 시간: 2022년 11월 10일, 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupFullAccess

설명: 이 정책은 백업 관리자를 위한 것으로, 백업 계획 생성 또는 편집, AWS 백업 계획에 AWS 리소스 할당, 백업 삭제, 백업 복원 등 백업 작업에 대한 모든 액세스 권한을 부여합니다.

AWSBackupFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBackupFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 18일, 22:21 UTC
- 편집 시간: 2023년 11월 27일 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
      "iam:GetResourceShareAssociations"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

설명: 사용자 대신 가상 머신의 메타데이터를 동기화할 수 있는 AWS BackupGateway 권한을 제공합니다.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 12월 15일, 19:43 UTC
- 편집된 시간: 2022년 12월 15일, 19:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupOperatorAccess

설명: 이 정책은 사용자에게 백업 계획에 AWS 리소스를 할당하고, 온디맨드 백업을 생성하고, 백업을 복원할 수 있는 권한을 부여합니다. 이 정책은 사용자가 백업 계획을 생성 또는 편집하도록 허용하거나 예약된 백업을 생성한 후 삭제하도록 허용하지 않습니다.

AWSBackupOperatorAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupOperatorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 18일, 22:23 UTC
- 편집된 시간: 2023년 9월 6일, 20:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "iam:GetResourceShareAssociations"
    ],
    "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupOrganizationAdminAccess

설명: 이 정책은 계정 간 백업 관리를 사용하여 조직의 백업을 관리하는 백업 관리자를 위한 것입니다.

AWSBackupOrganizationAdminAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupOrganizationAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 16:23 UTC
- 편집된 시간: 2022년 11월 18일, 18:26 UTC

- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}

```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupRestoreAccessForSAPHANA

설명: Amazon AWS EC2에서 SAP HANA의 백업을 복원할 수 있는 백업 권한을 제공합니다.

AWSBackupRestoreAccessForSAPHANA [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupRestoreAccessForSAPHANA를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 22:43 UTC
- 편집된 시간: 2022년 11월 10일, 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceLinkedRolePolicyForBackup

설명: 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 AWS Backup 권한을 제공합니다.

AWSBackupServiceLinkedRolePolicyForBackup [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 2일, 23:08 UTC
- 편집 시간: 2024년 5월 17일 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

정책 버전

정책 버전: v16(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Effect" : "Allow",
"Action" : [
  "elasticfilesystem:Backup",
  "elasticfilesystem:DescribeTags"
],
"Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
  }
}
},
{
  "Sid" : "DescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources",
    "elasticfilesystem:DescribeFileSystems",
    "dynamodb:ListTables",
    "storagegateway:ListVolumes",
    "ec2:DescribeVolumes",
    "ec2:DescribeInstances",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnapshotCopyTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
}
},
{
  "Sid" : "EC2CreateBackupTagPermissions",
```

```
"Effect" : "Allow",
"Action" : "ec2:CreateTags",
"Resource" : [
  "arn:aws:ec2:*::image/*",
  "arn:aws:ec2:*::snapshot/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AWSBackupManagedResource"
    ]
  }
}
},
{
  "Sid" : "EC2CreateTagsPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSBackupManagedResource" : "false"
    }
  }
},
{
  "Sid" : "EC2RDSDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeImages",
    "rds:DescribeDBSnapshots",
    "rds:DescribeDBClusterSnapshots"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EBSCopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
```

```
    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopyImage",
    "Resource" : "*"
  },
  {
    "Sid" : "EC2ModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeregisterImage",
      "ec2>DeleteSnapshot",
      "ec2:ModifySnapshotTier"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  },
  {
    "Sid" : "RDSInstanceAndSnashotPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:AddTagsToResource",
      "rds:CopyDBSnapshot",
      "rds>DeleteDBSnapshot",
      "rds>DeleteDBInstanceAutomatedBackup"
    ],
    "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
  },
  {
    "Sid" : "RDSClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:AddTagsToResource",
      "rds:CopyDBClusterSnapshot",
      "rds>DeleteDBClusterSnapshot"
    ],
    "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
  },
}
```

```
{
  "Sid" : "KMSDescribePermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSGrantPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListGrants",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "fsx.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "fsx.*.amazonaws.com"
      ]
    }
  }
},
{
```

```
"Sid" : "FsxPermissions",
"Effect" : "Allow",
"Action" : [
  "fsx:CopyBackup",
  "fsx:TagResource",
  "fsx:DescribeBackups",
  "fsx>DeleteBackup"
],
"Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
  "Sid" : "DynamoDBDeletePermissions",
  "Effect" : "Allow",
  "Action" : "dynamodb:DeleteBackup",
  "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
},
{
  "Sid" : "BackupGateway",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:ListVirtualMachines"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListTagsForBackupGateway",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:ListTagsForResource"
  ],
  "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
},
{
  "Sid" : "DynamoDBPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListTagsOfResource",
    "dynamodb:DescribeTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "StorageGatewayPermissions",
  "Effect" : "Allow",
```

```

    "Action" : [
      "storagegateway:DescribeCachediSCSIVolumes",
      "storagegateway:DescribeStorediSCSIVolumes"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "EventBridgePermissions",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:PutTargets",
      "events:DescribeRule",
      "events:EnableRule",
      "events:PutRule",
      "events:RemoveTargets",
      "events:ListTargetsByRule",
      "events:DisableRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
    ]
  },
  {
    "Sid" : "EventBridgeRulesPermissions",
    "Effect" : "Allow",
    "Action" : "events:ListRules",
    "Resource" : "*"
  },
  {
    "Sid" : "SSMSAPPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:GetOperation",
      "ssm-sap:UpdateHANABackupSettings"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TimestreamResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:ListDatabases",
      "timestream:ListTables",

```

```

    "timestream:ListTagsForResource",
    "timestream:DescribeDatabase",
    "timestream:DescribeTable",
    "timestream:GetAwsBackupStatus",
    "timestream:GetAwsRestoreStatus"
  ],
  "Resource" : [
    "arn:aws:timestream:*:*:database/*"
  ]
},
{
  "Sid" : "TimestreamPermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:DescribeEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RedshiftDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeTags"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/*",
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftClusterSnapshotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift>DeleteClusterSnapshot"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/*"
  ]
},
{
  "Sid" : "RedshiftClusterPermissions",
  "Effect" : "Allow",
  "Action" : [

```



```

    "redshift:DescribeClusters"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "CloudformationStackPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStacks"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/*"
  ]
},
{
  "Sid" : "RecoveryPointTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:TagResource"
  ],
  "Resource" : "arn:aws:backup:*:*:recovery-point:*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

설명: 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 백업 권한을 제공합니다 AWS .
 AWSBackupServiceLinkedRolePolicyForBackupTest [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 5월 12일, 17:37 UTC
- 편집된 시간: 2020년 5월 12일, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceRolePolicyForBackup

설명: 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 백업 권한을 제공합니다 AWS .

AWSBackupServiceRolePolicyForBackup [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForBackup를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 1월 10일, 21:01 UTC
- 편집 시간: 2024년 5월 17일 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AWSBackupServiceRolePolicyForBackup

정책 버전

정책 버전: v19(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb>DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
    },
  ],
}
```

```
"Resource" : "*"
},
{
  "Sid" : "RDSModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:ModifyDBInstance"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:*"
  ]
},
{
  "Sid" : "RDSClusterPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:ModifyDBCluster"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:cluster:*"
  ]
},
{
  "Sid" : "RDSClusterBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds>DeleteDBClusterAutomatedBackup"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
},
{
  "Sid" : "RDSBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds>DeleteDBSnapshot",
    "rds:ModifyDBSnapshotAttribute"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:snapshot:awsbackup:*"
  ]
},
{
  "Sid" : "RDSClusterModifyPermissions",
  "Effect" : "Allow",
```

```

    "Action" : [
      "rds:DeleteDBClusterSnapshot",
      "rds:ModifyDBClusterSnapshotAttribute"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    ]
  },
  {
    "Sid" : "StorageGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:CreateSnapshot",
      "storagegateway:ListTagsForResource"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "EBSCopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopySnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopyImage"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EBSTagAndDeletePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2Permissions",

```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateImage",
  "ec2:DeregisterImage",
  "ec2:DescribeSnapshots",
  "ec2:DescribeTags",
  "ec2:DescribeImages",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceCreditSpecifications",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeElasticGpus",
  "ec2:DescribeSpotInstanceRequests",
  "ec2:DescribeSnapshotTierStatus"
],
"Resource" : "*"
},
{
  "Sid" : "EC2TagPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:image/*"
},
{
  "Sid" : "EC2ModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotAttribute",
    "ec2:ModifyImageAttribute"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "EBSSnapshotTierPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotTier"
  ]
}
```

```

    ],
    "Resource" : "arn:aws:ec2:*::snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/aws:backup:source-resource" : "false"
      }
    }
  },
  {
    "Sid" : "BackupVaultPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup:DescribeBackupVault",
      "backup:CopyIntoBackupVault"
    ],
    "Resource" : "arn:aws:backup:*:*:backup-vault:*"
  },
  {
    "Sid" : "BackupVaultCopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup:CopyFromBackupVault"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EFSPermissions",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:Backup",
      "elasticfilesystem:DescribeTags"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
  },
  {
    "Sid" : "EBSResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeVolumes",
      "ec2:DescribeSnapshots"
    ],
    "Resource" : [

```



```
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "KMSDynamoDBPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "dynamodb.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSPermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
},
{
  "Sid" : "KMSSDataKeyEC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
```

```

    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "ec2.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "GetResourcesPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SSMSendPermissions",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Sid" : "FsxBackupPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DescribeBackups",
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  },
  {
    "Sid" : "FsxCreateBackupPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:CreateBackup",

```

```
"Resource" : [
  "arn:aws:fsx:*:*:file-system/*",
  "arn:aws:fsx:*:*:backup/*",
  "arn:aws:fsx:*:*:volume/*"
],
{
  "Sid" : "FsxPermissions",
  "Effect" : "Allow",
  "Action" : "fsx:DescribeFileSystems",
  "Resource" : "arn:aws:fsx:*:*:file-system/*"
},
{
  "Sid" : "FsxVolumePermissions",
  "Effect" : "Allow",
  "Action" : "fsx:DescribeVolumes",
  "Resource" : "arn:aws:fsx:*:*:volume/*"
},
{
  "Sid" : "FsxListTagsPermissions",
  "Effect" : "Allow",
  "Action" : "fsx:ListTagsForResource",
  "Resource" : [
    "arn:aws:fsx:*:*:file-system/*",
    "arn:aws:fsx:*:*:volume/*"
  ]
},
{
  "Sid" : "FsxDeletePermissions",
  "Effect" : "Allow",
  "Action" : "fsx>DeleteBackup",
  "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
  "Sid" : "FsxResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx:ListTagsForResource",
    "fsx:ManageBackupPrincipalAssociations",
    "fsx:CopyBackup",
    "fsx:TagResource"
  ],
  "Resource" : "arn:aws:fsx:*:*:backup/*"
},
}
```

```
{
  "Sid" : "DynamodbBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:StartAwsBackupJob",
    "dynamodb:ListTagsOfResource"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "BackupGatewayBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:Backup",
    "backup-gateway:ListTagsForResource"
  ],
  "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
},
{
  "Sid" : "CloudformationStackPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStacks",
    "cloudformation:GetTemplate",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
},
{
  "Sid" : "RedshiftCreatePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:CreateClusterSnapshot",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeTags"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/*",
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftSnapshotPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "redshift:DeleteClusterSnapshot"
],
"Resource" : [
  "arn:aws:redshift:*:*:snapshot:*/*"
]
},
{
  "Sid" : "RedshiftPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeClusters"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:CreateTags"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/*"
  ]
},
{
  "Sid" : "TimestreamResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:StartAwsBackupJob",
    "timestream:GetAwsBackupStatus",
    "timestream:ListTables",
    "timestream:ListDatabases",
    "timestream:ListTagsForResource",
    "timestream:DescribeTable",
    "timestream:DescribeDatabase"
  ],
  "Resource" : [
    "arn:aws:timestream:*:*:database/*"
  ]
},
}
```

```
{
  "Sid" : "TimestreamEndpointPermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:DescribeEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMSAPPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetOperation",
    "ssm-sap:ListDatabases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMSAPResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:BackupDatabase",
    "ssm-sap:UpdateHanaBackupSettings",
    "ssm-sap:GetDatabase",
    "ssm-sap:ListTagsForResource"
  ],
  "Resource" : "arn:aws:ssm-sap:*:*:*"
},
{
  "Sid" : "RecoveryPointTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:TagResource"
  ],
  "Resource" : "arn:aws:backup:*:*:recovery-point:*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceRolePolicyForRestores

설명: 여러 AWS 서비스에서 사용자를 대신하여 복원을 수행할 수 있는 AWS Backup 권한을 제공합니다. 이 정책에는 복원 프로세스의 일부인 EBS 볼륨, RDS 인스턴스, EFS 파일 시스템과 같은 AWS 리소스를 생성하고 삭제할 수 있는 권한이 포함됩니다.

AWSBackupServiceRolePolicyForRestores [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForRestores를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 1월 12일, 00:23 UTC
- 편집 시간: 2023년 12월 15일 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

정책 버전

정책 버전: v20(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceRolePolicyForS3Backup

설명: Backup이 모든 S3 버킷의 데이터를 AWS 백업하는 데 필요한 권한을 포함하는 정책입니다. 여기에는 모든 S3 객체에 대한 읽기 액세스와 모든 KMS 키에 대한 암호 해독 액세스가 포함됩니다.

AWSBackupServiceRolePolicyForS3Backup [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForS3Backup를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 18일, 17:40 UTC
- 편집 시간: 2024년 5월 17일 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBackupServiceRolePolicyForS3Restore

설명: Backup이 S3 AWS 백업을 버킷에 복원하는 데 필요한 권한을 포함하는 정책입니다. 여기에는 모든 S3 버킷에 대한 읽기/쓰기 권한, 모든 KMS 키에 대한 권한 및 모든 KMS DescribeKey 키에 대한 권한이 포함됩니다. GenerateDataKey

AWSBackupServiceRolePolicyForS3Restore [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForS3Restore를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 18일, 17:39 UTC
- 편집된 시간: 2023년 2월 7일, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBatchFullAccess

설명: AWS Batch 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSBatchFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBatchFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 6일, 19:35 UTC
- 편집된 시간: 2022년 10월 24일, 16:09 UTC
- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBatchServiceEventTargetRole

설명: AWS Batch Job 제출을 위한 CloudWatch 이벤트 대상을 활성화하는 정책

AWSBatchServiceEventTargetRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBatchServiceEventTargetRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 2월 28일, 22:31 UTC
- 편집된 시간: 2018년 2월 28일, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBatchServiceRole

설명: EC2, 오토스케일링, EC2 컨테이너 서비스 및 Cloudwatch 로그를 비롯한 관련 서비스에 대한 액세스를 허용하는 AWS Batch 서비스 역할에 대한 정책입니다.

AWSBatchServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBatchServiceRole을 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 6일, 19:36 UTC
- 편집 시간: 2023년 12월 5일 18:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBCMDataExportsServiceRolePolicy

설명: Billing and Cost Management 데이터를 제공하는 AWS 서비스 연결 역할은 고객을 대신하여 Amazon S3와 같은 대상 위치로 데이터를 내보내기 위한 서비스 데이터에 대한 액세스 권한을 내보냅니다.

AWSBCMDataExportsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 6월 10일 17:40 UTC
- 편집 시간: 2024년 6월 10일 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
```

```
    "cost-optimization-hub:ListRecommendations"
  ],
  "Resource" : "*"
}
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBillingConductorFullAccess

설명: AWSBillingConductorFullAccess 관리형 정책을 사용하여 AWS Billing Conductor (ABC) 콘솔 및 API에 대한 전체 액세스를 허용하십시오. 이 정책을 통해 사용자는 ABC 리소스를 나열, 생성 및 삭제할 수 있습니다.

AWSBillingConductorFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingConductorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 13일, 18:02 UTC
- 편집된 시간: 2022년 4월 13일, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBillingConductorReadOnlyAccess

설명: AWSBillingConductorReadOnlyAccess 관리형 정책을 사용하여 AWS Billing Conductor (ABC) 콘솔 및 API에 대한 읽기 전용 액세스를 허용하세요. 이 정책은 모든 ABC 리소스를 보고 나열할 수 있는 권한을 부여합니다. 리소스를 생성 또는 삭제하는 기능은 포함되지 않습니다.

AWSBillingConductorReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingConductorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 4월 13일, 18:02 UTC
- 편집된 시간: 2022년 4월 13일, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBillingReadOnlyAccess

설명: 사용자가 결제 콘솔에서 청구서를 볼 수 있습니다.

AWSBillingReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 27일, 20:08 UTC
- 편집 시간: 2024년 5월 23일 23:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

설명: 이 정책은 AWS 리소스를 제어할 권한을 부여합니다. 예를 들어 AWS Systems Manager (SSM) 스크립트를 실행하여 EC2 또는 RDS 인스턴스를 시작하고 중지할 수 있습니다.

[AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#) [관리형 정책입니다.](#)
[다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에

[AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#)를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 5월 25일, 19:03 UTC
- 편집된 시간: 2022년 5월 25일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBudgetsActionsWithAWSResourceControlAccess

설명: AWS 예산 조치를 사용하여 실행 중인 AWS 리소스의 상태를 제어하는 것을 포함하여 예산 작업에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBudgetsActionsWithAWSResourceControlAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 15일, 17:19 UTC
- 편집된 시간: 2020년 10월 15일, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBudgetsReadOnlyAccess

설명: 를 통해 AWS 예산 콘솔에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AWSBudgetsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBudgetsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 15일, 17:18 UTC
- 편집된 시간: 2020년 10월 15일, 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBugBustFullAccess

설명: 이 IAM 정책은 사용자에게 콘솔에 대한 전체 액세스 권한을 부여합니다 AWS BugBust .

AWSBugBustFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSBugBustFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 6월 24일, 07:03 UTC
- 편집된 시간: 2021년 7월 22일, 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBugBustPlayerAccess

설명: 이 IAM 정책은 사용자에게 이벤트 참여 AWS BugBust 권한을 부여합니다.

AWSBugBustPlayerAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBugBustPlayerAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 6월 24일, 07:15 UTC
- 편집된 시간: 2021년 6월 24일, 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSBugBustServiceRolePolicy

설명: 사용자 대신 AWS BugBust 리소스에 액세스할 수 있는 권한을 부여합니다.

AWSBugBustServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 24일, 06:59 UTC

- 편집된 시간: 2021년 6월 24일, 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerFullAccess

설명: AWS 인증서 관리자 (ACM) 에 대한 전체 액세스 권한 제공

AWSCertificateManagerFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 21일, 17:02 UTC
- 편집된 시간: 2020년 8월 17일, 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerPrivateCAAuditor

설명: 감사자에게 AWS Certificate Manager 사설 인증 기관에 대한 액세스 권한을 제공합니다.

AWSCertificateManagerPrivateCAAuditor [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAAuditor를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:51 UTC
- 편집된 시간: 2020년 8월 17일, 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerPrivateCAFullAccess

설명: AWS Certificate Manager 사설 인증 기관에 대한 전체 액세스 권한을 제공합니다.

AWSCertificateManagerPrivateCAFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:54 UTC
- 편집된 시간: 2018년 10월 23일, 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerPrivateCAPrivilegedUser

설명: 인증서 관리자 사설 인증 기관에 대한 권한 있는 AWS 인증서 사용자 액세스를 제공합니다.

AWSCertificateManagerPrivateCAPrivilegedUser [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAPrivilegedUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 20일, 17:43 UTC
- 편집된 시간: 2019년 6월 20일, 17:43 UTC

- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerPrivateCAReadOnly

설명: AWS Certificate Manager 사설 인증 기관에 대한 읽기 전용 액세스를 제공합니다.

AWSCertificateManagerPrivateCAReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 10월 23일, 16:57 UTC
- 편집된 시간: 2020년 8월 17일, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerPrivateCAUser

설명: 인증서 사용자에게 Certificate Manager 사설 AWS 인증 기관에 대한 액세스 권한을 제공합니다.

AWSCertificateManagerPrivateCAUser [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:53 UTC
- 편집된 시간: 2019년 6월 20일, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCertificateManagerReadOnly

설명: AWS 인증서 관리자 (ACM) 에 대한 읽기 전용 액세스를 제공합니다.

AWSCertificateManagerReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 21일, 17:07 UTC
- 편집된 시간: 2021년 3월 15일, 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",

```

```

    "acm:ListTagsForCertificate",
    "acm:GetAccountConfiguration"
  ],
  "Resource" : "*"
}
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSChatbotServiceLinkedRolePolicy

설명: AWS Chatbot이 사용하는 서비스 연결 역할입니다.

AWSChatbotServiceLinkedRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 18일, 16:39 UTC
- 편집된 시간: 2019년 11월 18일, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCleanRoomsFullAccess

설명: AWS Clean Rooms 리소스에 대한 전체 액세스 권한 및 관련 리소스에 대한 액세스를 허용합니다. AWS 서비스.

AWSCleanRoomsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:10 UTC
- 편집 시간: 2024년 3월 21일 15:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCleanRoomsFullAccessNoQuerying

설명: 공동 작업에서의 쿼리 및 관련 리소스에 대한 액세스를 제외하고 AWS Clean Rooms 리소스에 대한 전체 액세스를 허용합니다. AWS 서비스

AWSCleanRoomsFullAccessNoQuerying [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsFullAccessNoQuerying를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:12 UTC
- 편집 시간: 2024년 5월 14일 18:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCleanRoomsMLFullAccess

설명: AWS Clean Rooms ML 리소스에 대한 전체 액세스 권한과 관련 리소스에 대한 액세스를 허용합니다 AWS 서비스.

AWSCleanRoomsMLFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsMLFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 29일 21:02 UTC
- 편집 시간: 2023년 11월 29일, 21:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCleanRoomsMLReadOnlyAccess

설명: AWS Clean Rooms ML 리소스에 대한 읽기 전용 액세스 및 관련 AWS 클린 룸 리소스에 대한 읽기 전용 액세스를 허용합니다.

AWSCleanRoomsMLReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsMLReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 29일 20:55 UTC
- 편집 시간: 2023년 11월 29일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCleanRoomsReadOnlyAccess

설명: AWS Clean Rooms 리소스에 대한 읽기 전용 액세스와 관련 AWS Glue 및 Amazon CloudWatch Logs 리소스에 대한 읽기 전용 액세스를 허용합니다.

AWSCleanRoomsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:10 UTC
- 편집된 시간: 2023년 1월 12일, 16:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloud9Administrator

설명: 관리자에게 AWS Cloud9에 대한 액세스 권한을 제공합니다.

AWSCloud9Administrator [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloud9Administrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:17 UTC
- 편집된 시간: 2023년 10월 11일, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```



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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloud9EnvironmentMember

설명: AWS Cloud9 공유 개발 환경에 초대받을 수 있는 기능을 제공합니다.

AWSCloud9EnvironmentMember [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloud9EnvironmentMember를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:18 UTC
- 편집된 시간: 2023년 10월 11일, 12:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloud9ServiceRolePolicy

설명: AWS Cloud9용 서비스 연결 역할 정책

AWSCloud9ServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2017년 11월 30일, 13:44 UTC
- 편집된 시간: 2022년 1월 17일, 14:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloud9SSMInstanceProfile

설명: 이 정책은 Cloud9가 SSM 세션 관리자를 사용하여 인스턴스에 연결할 수 있도록 하는 역할을 연결하는 데 사용됩니다. InstanceProfile

AWSCloud9SSMInstanceProfile [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCloud9SSMInstanceProfile를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 14일, 11:40 UTC
- 편집된 시간: 2020년 5월 14일, 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloud9User

설명: AWS Cloud9 개발 환경을 생성하고 소유 환경을 관리할 수 있는 권한을 제공합니다.

AWSCloud9User [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloud9User를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:16 UTC
- 편집된 시간: 2023년 10월 11일, 13:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  ]
}

```

```
    ]  
  }  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudFormationFullAccess

설명: 에 대한 전체 액세스 권한을 제공합니다 AWS CloudFormation.

AWSCloudFormationFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudFormationFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 26일, 21:50 UTC
- 편집된 시간: 2019년 7월 26일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudFormationReadOnlyAccess

설명: AWS CloudFormation 를 통해 액세스를 제공합니다 AWS Management Console.

AWSCloudFormationReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudFormationReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2019년 11월 13일, 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWS CloudFrontLogger

설명: CloudFront 로거에 CloudWatch 로그에 쓰기 권한을 부여합니다.

AWSCloudFrontLogger [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 12일, 20:15 UTC
- 편집된 시간: 2019년 11월 22일, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudHSMFullAccess

설명: 모든 CloudHSM 리소스에 대한 전체 액세스를 제공합니다.

AWSCloudHSMFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudHSMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudHSMReadOnlyAccess

설명: 모든 CloudHSM 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSCloudHSMReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudHSMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudHSMRole

설명: AWS CloudHSM 서비스 역할에 대한 기본 정책입니다.

AWSCloudHSMRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudHSMRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudMapDiscoverInstanceAccess

설명: AWS 클라우드 맵 디스커버리 API에 대한 액세스를 제공합니다.

AWSCloudMapDiscoverInstanceAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapDiscoverInstanceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 00:02 UTC
- 편집된 시간: 2023년 9월 20일, 21:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudMapFullAccess

설명: 모든 AWS 클라우드 맵 작업에 대한 전체 액세스 권한을 제공합니다.

AWSCloudMapFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 23:57 UTC
- 편집된 시간: 2020년 7월 29일, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudMapReadOnlyAccess

설명: 모든 AWS 클라우드 맵 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSCloudMapReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 23:45 UTC
- 편집된 시간: 2023년 9월 20일, 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudMapRegisterInstanceAccess

설명: AWS 클라우드 맵 작업에 등록자 수준의 액세스 권한을 제공합니다.

AWSCloudMapRegisterInstanceAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapRegisterInstanceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 00:04 UTC
- 편집된 시간: 2023년 9월 20일, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudShellFullAccess

설명: 모든 기능과 AWS CloudShell 함께 사용할 수 있는 권한을 부여합니다.

AWSCloudShellFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudShellFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:07 UTC
- 편집된 시간: 2020년 12월 15일, 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudTrail_FullAccess

설명: 에 대한 전체 액세스 권한을 제공합니다 AWS CloudTrail.

AWSCloudTrail_FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudTrail_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 8일, 23:41 UTC
- 편집된 시간: 2021년 2월 22일, 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudTrail_ReadOnlyAccess

설명: 에 대한 읽기 전용 액세스를 제공합니다 AWS CloudTrail.

AWSCloudTrail_ReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudTrail_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 6월 14일, 17:19 UTC
- 편집된 시간: 2022년 6월 14일, 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

설명: 이 정책은 이라는 서비스 연결 역할이 사용합니다.

AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents CloudWatch 이 서비스 연결 역할을 사용하여 CloudWatch 경보가 ALARM 상태로 전환될 때 AWS System Manager 인시던트 관리자 작업을 수행합니다. 이 정책은 사용자를 대신하여 인시던트를 시작할 수 있는 권한을 부여합니다.

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 27일, 13:30 UTC
- 편집된 시간: 2021년 4월 27일, 13:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeArtifactAdminAccess

설명: AWS CodeArtifact 를 통해 전체 액세스 권한을 제공합니다 AWS Management Console.

AWSCodeArtifactAdminAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeArtifactAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 16일, 23:53 UTC
- 편집된 시간: 2020년 6월 16일, 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeArtifactReadOnlyAccess

설명: AWS CodeArtifact 를 통해 읽기 전용 액세스를 제공합니다 AWS Management Console.

AWSCodeArtifactReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeArtifactReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 25일, 21:23 UTC
- 편집된 시간: 2020년 6월 25일, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeBuildAdminAccess

설명: AWS CodeBuild 를 통해 전체 액세스 권한을 제공합니다 AWS Management Console. 또한 ReadOnlyAccess AmazonS3를 연결하여 빌드 아티팩트를 다운로드할 수 있는 액세스를 제공하고, FullAccess IAM을 연결하여 서비스 역할을 생성 및 관리할 수 있습니다. CodeBuild

AWSCodeBuildAdminAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:04 UTC
- 편집 시간: 2024년 5월 2일 01:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
```

```

    "codecommit:ListRepositories",
    "cloudwatch:GetMetricStatistics",
    "ec2:DescribeVpcs",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ecr:DescribeRepositories",
    "ecr:ListImages",
    "elasticfilesystem:DescribeFileSystems",
    "events:DeleteRule",
    "events:DescribeRule",
    "events:DisableRule",
    "events:EnableRule",
    "events:ListTargetsByRule",
    "events:ListRuleNamesByTarget",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "logs:GetLogEvents",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "CWLDeleteLogGroupAccess",
  "Action" : [
    "logs:DeleteLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [

```

```

    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:CreateConnection",
    "codestar-connections>DeleteConnection",
    "codestar-connections:UpdateConnectionInstallation",
    "codestar-connections:TagResource",
    "codestar-connections:UntagResource",
    "codestar-connections:ListConnections",
    "codestar-connections:ListInstallationTargets",
    "codestar-connections:ListTagsForResource",
    "codestar-connections:GetConnection",
    "codestar-connections:GetIndividualAccessToken",
    "codestar-connections:GetInstallationUrl",
    "codestar-connections:PassConnection",
    "codestar-connections:StartOAuthHandshake",
    "codestar-connections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "CodeStarNotificationsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListEventTypes",
      "codestar-notifications:ListTargets",
      "codestar-notifications:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:SetTopicAttributes"
    ],
    "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
  },
  {
    "Sid" : "SNSTopicListAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics",
      "sns:GetTopicAttributes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CodeStarNotificationsChatbotAccess",
    "Effect" : "Allow",
    "Action" : [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ],
    "Resource" : "*"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeBuildDeveloperAccess

설명: AWS CodeBuild 를 통해 액세스를 AWS Management Console에 제공하지만 CodeBuild 프로젝트 관리는 허용하지 않습니다. 또한 ReadOnlyAccess AmazonS3를 연결하여 빌드 아티팩트를 다운로드 할 수 있는 액세스 권한을 제공하십시오.

AWSCodeBuildDeveloperAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildDeveloperAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:02 UTC
- 편집 시간: 2024년 5월 2일 01:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```



```
"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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeBuildReadOnlyAccess

설명: AWS CodeBuild 를 통해 읽기 전용 액세스를 제공합니다 AWS Management Console. 또한 ReadOnlyAccess AmazonS3를 연결하여 빌드 아티팩트를 다운로드할 수 있는 액세스 권한을 제공하십시오.

AWSCodeBuildReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:03 UTC
- 편집 시간: 2024년 5월 2일 01:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeCommitFullAccess

설명: AWS CodeCommit 를 통해 전체 액세스 권한을 제공합니다 AWS Management Console.

AWSCodeCommitFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeCommitFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:02 UTC
- 편집된 시간: 2023년 7월 17일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeCommitPowerUser

설명: 리포지토리에 대한 전체 액세스를 제공하지만 AWS CodeCommit 리포지토리 삭제는 허용하지 않습니다.

AWSCodeCommitPowerUser [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeCommitPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:06 UTC
- 편집된 시간: 2023년 7월 17일, 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeCommitReadOnly

설명: AWS CodeCommit 를 통해 읽기 전용 액세스를 제공합니다 AWS Management Console.

AWSCodeCommitReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeCommitReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:05 UTC
- 편집된 시간: 2021년 8월 18일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployDeployerAccess

설명: 개정판을 등록하고 배포할 수 있는 액세스 권한을 제공합니다.

AWSCodeDeployDeployerAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployDeployerAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:18 UTC
- 편집된 시간: 2020년 4월 2일, 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployFullAccess

설명: CodeDeploy 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSCodeDeployFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeDeployFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:13 UTC
- 편집된 시간: 2020년 4월 2일, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployReadOnlyAccess

설명: CodeDeploy 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSCodeDeployReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:21 UTC
- 편집된 시간: 2020년 4월 2일, 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRole

설명: 사용자를 대신하여 태그를 확장하고 Auto Scaling과 상호 작용할 수 있는 CodeDeploy 서비스 액세스를 제공합니다.

AWSCodeDeployRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 4일, 18:05 UTC
- 편집된 시간: 2023년 8월 16일, 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRoleForCloudFormation

설명: 사용자 대신 Lambda 함수를 호출하여 블루/그린 배포를 수행할 수 있는 CodeDeploy 서비스 액세스를 제공합니다. CloudFormation

AWSCodeDeployRoleForCloudFormation [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForCloudFormation를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 5월 19일, 17:12 UTC
- 편집된 시간: 2020년 5월 19일, 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRoleForECS

설명: 사용자를 대신하여 ECS 블루/그린 배포를 수행할 수 있는 CodeDeploy 서비스 전체 액세스를 제공합니다. 모든 S3 객체 읽기, 모든 Lambda 함수 호출, 계정 내 모든 SNS 주제에 게시, 모든 ECS 서비스 업데이트에 대한 전체 액세스와 같은 지원 서비스에 대한 전체 액세스를 부여합니다.

AWSCodeDeployRoleForECS [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForECS를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 20:40 UTC
- 편집된 시간: 2019년 9월 23일, 22:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    ]
  }
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRoleForECSLimited

설명: 사용자를 대신하여 ECS 블루/그린 배포를 수행할 수 있는 CodeDeploy 서비스 제한 액세스를 제공합니다.

AWSCodeDeployRoleForECSLimited [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForECSLimited를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 20:42 UTC
- 편집된 시간: 2019년 9월 23일, 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRoleForLambda

설명: 사용자를 대신하여 Lambda 배포를 수행할 수 있는 CodeDeploy 서비스 액세스를 제공합니다.

AWSCodeDeployRoleForLambda [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForLambda를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 28일, 14:05 UTC
- 편집된 시간: 2019년 12월 3일, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeDeployRoleForLambdaLimited

설명: 사용자를 대신하여 Lambda 배포를 수행할 수 있는 CodeDeploy 서비스 제한 액세스를 제공합니다.

AWSCodeDeployRoleForLambdaLimited [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForLambdaLimited를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 17일, 17:14 UTC
- 편집된 시간: 2020년 8월 17일, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodePipeline_FullAccess

설명: AWS CodePipeline 를 통해 전체 액세스 권한을 제공합니다 AWS Management Console.

AWSCodePipeline_FullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipeline_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 3일, 22:38 UTC
- 편집 시간: 2024년 3월 14일 17:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodePipeline_ReadOnlyAccess

설명: AWS CodePipeline 를 통해 읽기 전용 액세스를 제공합니다 AWS Management Console.

AWSCodePipeline_ReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipeline_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 3일, 22:25 UTC
- 편집된 시간: 2020년 8월 3일, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodePipelineApproverAccess

설명: 모든 파이프라인의 수동 변경을 보고 승인할 수 있는 액세스 권한을 제공합니다.

AWSCodePipelineApproverAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipelineApproverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 7월 28일, 18:59 UTC
- 편집된 시간: 2017년 8월 2일, 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodePipelineCustomActionAccess

설명: 작업 세부 정보 (임시 자격 증명 포함) 를 폴링하고 상태 업데이트를 보고하기 위한 사용자 지정 작업에 대한 액세스를 제공합니다 AWS CodePipeline.

AWSCodePipelineCustomActionAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipelineCustomActionAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:02 UTC
- 편집된 시간: 2015년 7월 9일, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeStarFullAccess

설명: AWS CodeStar 를 통해 전체 액세스 권한을 제공합니다 AWS Management Console.

AWSCodeStarFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeStarFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 19일, 16:23 UTC
- 편집된 시간: 2023년 3월 28일, 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeStarNotificationsServiceRolePolicy

설명: AWS CodeStar 알림이 사용자를 대신하여 Amazon CloudWatch Events에 액세스할 수 있도록 허용합니다.

AWSCodeStarNotificationsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 5일, 16:10 UTC
- 편집된 시간: 2020년 3월 19일, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCodeStarServiceRole

설명: 사용하지 마세요 - AWS CodeStar 고객을 대신하여 IAM 및 기타 서비스 리소스를 관리할 수 있는 관리 권한을 부여하는 서비스 역할 정책. CodeStar

AWSCodeStarServiceRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeStarServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 4월 19일, 15:20 UTC
- 편집된 시간: 2021년 9월 20일, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCompromisedKeyQuarantine

설명: IAM 사용자의 자격 증명에 침해되거나 공개적으로 노출된 경우 AWS 팀에서 적용하는 특정 작업에 대한 액세스를 거부합니다. 이 정책을 삭제하지 마십시오. 대신, 이 이벤트와 관련하여 전송된 이메일에 명시된 지침을 따르세요.

AWSCompromisedKeyQuarantine [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSCompromisedKeyQuarantine를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 11일, 18:04 UTC
- 편집된 시간: 2020년 8월 11일, 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCompromisedKeyQuarantineV2

설명: IAM 사용자의 자격 증명이 침해되거나 공개적으로 노출된 경우 AWS 팀에서 적용하는 특정 작업에 대한 액세스를 거부합니다. 이 정책을 삭제하지 마십시오. 대신 이 이벤트와 관련하여 생성된 지원 사례에 명시된 지침을 따르세요.

AWSCompromisedKeyQuarantineV2 [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCompromisedKeyQuarantineV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 21일, 22:30 UTC
- 편집된 시간: 2023년 3월 16일, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigMultiAccountSetupPolicy

설명: Config가 AWS 서비스를 호출하고 조직 전체에 구성 리소스를 배포할 수 있도록 허용합니다.

AWSConfigMultiAccountSetupPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 17일, 18:03 UTC
- 편집된 시간: 2023년 2월 24일, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigRemediationServiceRolePolicy

설명: AWS Config가 사용자 대신 규정을 준수하지 않는 리소스를 수정할 수 있도록 허용합니다.

AWSConfigRemediationServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 18일, 21:21 UTC
- 편집된 시간: 2019년 6월 18일, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigRoleForOrganizations

설명: AWS Config가 읽기 전용 AWS Organizations API를 호출하도록 허용합니다.

AWSConfigRoleForOrganizations [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSConfigRoleForOrganizations를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 3월 19일, 22:53 UTC
- 편집된 시간: 2020년 11월 24일, 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigRulesExecutionRole

설명: AWS Lambda 함수가 AWS Config API 및 Config가 Amazon S3에 정기적으로 전송하는 구성 스냅샷에 액세스할 수 있도록 AWS 허용합니다. 이 액세스는 사용자 지정 Config 규칙에 대한 구성 변경을 평가하는 함수에 필요합니다.

AWSConfigRulesExecutionRole [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSConfigRulesExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 3월 25일, 17:59 UTC
- 편집된 시간: 2019년 5월 13일, 21:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigServiceRolePolicy

설명: Config가 사용자를 대신하여 AWS 서비스를 호출하고 리소스 구성을 수집할 수 있도록 허용합니다.

AWSConfigServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 30일, 23:31 UTC
- 편집 시간: 2024년 2월 22일 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

정책 버전

정책 버전: v50(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConfigUserAccess

설명: 리소스의 태그별 검색, 모든 태그 읽기 등 AWS Config를 사용할 수 있는 액세스 권한을 제공합니다. 이는 관리자 권한이 필요한 AWS Config를 구성할 수 있는 권한을 제공하지 않습니다.

AWSConfigUserAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSConfigUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 18일, 19:38 UTC
- 편집된 시간: 2019년 3월 18일, 20:27 UTC

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

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSConnector

설명: Connector가 사용자를 대신하여 VM을 가져올 수 있도록 모든 EC2 객체에 대한 광범위한 읽기/쓰기 액세스, 'import-to-ec2-'로 시작하는 S3 버킷에 대한 읽기/쓰기 액세스, 모든 S3 버킷을 나열하는 기능을 활성화합니다. AWS

AWSConnector [관리형 정책입니다AWS](#).

이 정책 사용

사용자, 그룹 및 역할에 AWSConnector를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 11일, 17:14 UTC
- 편집된 시간: 2015년 9월 28일, 19:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSControlTowerAccountServiceRolePolicy

설명: AWS Control Tower가 사용자를 대신하여 자동화된 계정 구성 및 중앙 집중식 거버넌스를 제공하는 AWS 서비스를 호출할 수 있습니다.

AWSControlTowerAccountServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 5일, 22:04 UTC
- 편집된 시간: 2023년 6월 5일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSControlTowerServiceRolePolicy

설명: AWS Control Tower에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

AWSControlTowerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSControlTowerServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 5월 3일, 18:19 UTC
- 편집된 시간: 2023년 4월 12일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSCostAndUsageReportAutomationPolicy

설명: 계정 구성을 설명하고, MAP 프로그램용 S3 버킷을 생성하여 여기에 태그를 적용하고, 비용 및 사용 보고서를 생성하고, 비용 및 사용 보고서 정의를 설명할 수 있는 권한을 부여합니다.

AWSCostAndUsageReportAutomationPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSCostAndUsageReportAutomationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 1일, 21:27 UTC
- 편집된 시간: 2021년 11월 1일, 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataExchangeFullAccess

설명: 및 SDK를 사용하는 AWS Data Exchange 및 AWS Marketplace 작업에 대한 전체 액세스 권한을 부여합니다 AWS Management Console . 또한 AWS Data Exchange를 최대한 활용하는 데 필요한 관련 서비스에 대한 선별된 액세스를 제공합니다.

AWSDataExchangeFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDataExchangeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집 시간: 2024년 5월 7일 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataExchangeProviderFullAccess

설명: 데이터 공급자에게 및 SDK를 사용하는 AWS Data Exchange 및 AWS Marketplace 작업에 대한 액세스 권한을 부여합니다 AWS Management Console . 또한 AWS Data Exchange를 최대한 활용하는 데 필요한 관련 서비스에 대한 선별된 액세스를 제공합니다.

AWSDataExchangeProviderFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDataExchangeProviderFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2022년 3월 15일, 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataExchangeReadOnly

설명: 및 SDK를 사용하는 AWS Data Exchange 및 AWS Marketplace 작업에 대한 읽기 전용 액세스 권한을 부여합니다 AWS Management Console .

AWSDataExchangeReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDataExchangeReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2021년 5월 10일, 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataExchangeSubscriberFullAccess

설명: 데이터 구독자에게 AWS Data Exchange에 대한 액세스 권한과 AWS Management Console 및 SDK를 사용한 AWS Marketplace 작업을 부여합니다. 또한 AWS Data Exchange를 최대한 활용하는데 필요한 관련 서비스에 대한 선별된 액세스를 제공합니다.

AWSDataExchangeSubscriberFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDataExchangeSubscriberFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집 시간: 2024년 5월 21일 17:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataLifecycleManagerServiceRole

설명: AWS 데이터 라이프사이클 관리자가 AWS 리소스에 대한 조치를 취할 수 있는 적절한 권한을 제공합니다.

AWSDataLifecycleManagerServiceRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDataLifecycleManagerServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 7월 6일, 19:34 UTC
- 편집된 시간: 2022년 9월 19일, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

설명: AMI Management용 AWS 리소스에 대해 조치를 취할 수 있는 적절한 권한을 AWS 데이터 라이프사이클 관리자에게 제공합니다.

AWSDataLifecycleManagerServiceRoleForAMIManagement [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDataLifecycleManagerServiceRoleForAMIManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 10월 21일, 19:39 UTC
- 편집된 시간: 2021년 8월 19일, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDatalifecycleManagerSSMFullAccess

설명: 모든 Amazon EC2 인스턴스에서 사전 및 사후 스크립트를 실행하는 데 필요한 Systems Manager 작업을 수행할 수 있는 Amazon Data Lifecycle Manager 권한을 제공합니다.

AWSDatalifecycleManagerSSMFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDatalifecycleManagerSSMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 31일, 20:29 UTC
- 편집 시간: 2023년 11월 16일 22:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDatalifecycleManagerSSMFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDatapipeline_FullAccess

설명: 데이터 파이프라인에 대한 전체 액세스, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 액세스 목록, 기본 역할에 대한 PassRole 액세스를 제공합니다.

AWSDatapipeline_FullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDatapipeline_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 1월 19일, 23:14 UTC
- 편집된 시간: 2017년 8월 17일, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataPipeline_PowerUser

설명: 데이터 파이프라인에 대한 전체 액세스, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 액세스 목록, 기본 역할에 대한 PassRole 액세스를 제공합니다.

AWSDataPipeline_PowerUser [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDataPipeline_PowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 19일, 23:16 UTC
- 편집된 시간: 2017년 8월 17일, 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataSyncDiscoveryServiceRolePolicy

설명: DataSync Discovery가 사용자를 대신하여 다른 AWS 서비스와 통합할 수 있도록 허용합니다.

AWSDataSyncDiscoveryServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 20일, 22:19 UTC
- 편집된 시간: 2023년 3월 20일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataSyncFullAccess

설명: 종속성에 대한 전체 액세스 AWS DataSync 권한과 종속성에 대한 최소 액세스를 제공합니다.

AWSDataSyncFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDataSyncFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 19:40 UTC
- 편집 시간: 2024년 2월 16일 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDataSyncReadOnlyAccess

설명: 에 대한 읽기 전용 액세스를 제공합니다. AWS DataSync

AWSDataSyncReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDataSyncReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 19:18 UTC
- 편집된 시간: 2020년 6월 30일, 17:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-FleetWorker

설명: AWS Deadline Cloud 작업자에게 팜에서 작업을 실행할 수 있는 액세스 권한을 제공합니다.

AWSDeadlineCloud-FleetWorker [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-FleetWorker를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 17:21 UTC
- 편집 시간: 2024년 4월 1일 17:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-UserAccessFarms

설명: 다른 필수 서비스를 호출할 수 있는 제한된 읽기 전용 권한으로 AWS Deadline Cloud 팜에 대한 사용자 워크스테이션 액세스를 제공합니다. 스튜디오와 관련된 사용자 역할에 이 정책을 추가하세요.

AWSDeadlineCloud-UserAccessFarms [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-UserAccessFarms를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 16:54 UTC
- 편집 시간: 2024년 4월 1일 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
      }
    }
  }
}

```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-UserAccessFleets

설명: 다른 필수 서비스를 호출할 수 있도록 제한된 읽기 전용 권한으로 AWS Deadline Cloud 플릿에 대한 사용자 워크스테이션 액세스를 제공합니다. 스튜디오와 관련된 사용자 역할에 이 정책을 첨부하세요.

AWSDeadlineCloud-UserAccessFleets [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-UserAccessFleets를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 17:01 UTC
- 편집 시간: 2024년 4월 1일 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-UserAccessJobs

설명: 다른 필수 서비스를 호출할 수 있는 제한된 읽기 전용 권한으로 AWS Deadline Cloud 작업에 대한 사용자 워크스테이션 액세스를 제공합니다. 스튜디오와 관련된 사용자 역할에 이 정책을 첨부하세요.

AWSDeadlineCloud-UserAccessJobs [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-UserAccessJobs를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 17:05 UTC
- 편집 시간: 2024년 4월 1일 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-UserAccessQueues

설명: 다른 필수 서비스를 호출할 수 있도록 제한된 읽기 전용 권한으로 AWS Deadline Cloud 대기열에 대한 사용자 워크스테이션 액세스를 제공합니다. 스튜디오와 관련된 사용자 역할에 이 정책을 추가하세요.

AWSDeadlineCloud-UserAccessQueues [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-UserAccessQueues를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 17:10 UTC
- 편집 시간: 2024년 4월 1일 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeadlineCloud-WorkerHost

설명: AWS Deadline Cloud 작업자 호스트가 팜의 플릿에 참여할 수 있는 액세스 권한을 제공합니다.

AWSDeadlineCloud-WorkerHost [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeadlineCloud-WorkerHost를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 4월 1일 17:28 UTC
- 편집 시간: 2024년 4월 1일 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
```

```

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepLensLambdaFunctionAccessPolicy

설명: 이 정책은 디바이스에서 실행되는 DeepLens 관리 람다 함수에 필요한 권한을 지정합니다.
DeepLens

AWSDeepLensLambdaFunctionAccessPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepLensLambdaFunctionAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 15:47 UTC
- 편집된 시간: 2019년 6월 11일, 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepLensServiceRolePolicy

설명: IoT, S3 AWS 서비스, GreenGrass AWS Lambda를 비롯한 종속성에 필요한 리소스 DeepLens 및 역할에 대한 AWS DeepLens 액세스 권한을 부여합니다.

AWSDeepLensServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepLensServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 29일, 15:46 UTC
- 편집된 시간: 2019년 9월 25일, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerAccountAdminAccess

설명: DeepRacer 관리자는 다중 사용자 모드와 단일 사용자 모드 간 전환을 포함한 모든 작업에 액세스할 수 있습니다.

AWSDeepRacerAccountAdminAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerAccountAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 28일, 01:27
- 편집된 시간: 2021년 10월 28일, 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerCloudFormationAccessPolicy

설명: 사용자 대신 AWS 스택과 리소스를 생성하고 관리할 수 있습니다. CloudFormation

AWSDeepRacerCloudFormationAccessPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 `AWSDeepRacerCloudFormationAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 2월 28일, 21:59 UTC
- 편집된 시간: 2019년 6월 14일, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerDefaultMultiUserAccess

설명: 다중 사용자 모드에서 deepracer를 사용하기 위한 DeepRacer MultiUser 기본 사용자 액세스 권한

AWSDeepRacerDefaultMultiUserAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerDefaultMultiUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 28일, 01:27
- 편집된 시간: 2021년 10월 28일, 01:27 UTC

- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "depracer:Add*",
        "depracer:Remove*",
        "depracer:Create*",
        "depracer:Perform*",
        "depracer:Clone*",
        "depracer:Get*",
        "depracer:List*",
        "depracer>Edit*",
        "depracer:Start*",
        "depracer:Set*",
        "depracer:Update*",
        "depracer>Delete*",
        "depracer:Stop*",
        "depracer:Import*",
        "depracer:Tag*",
        "depracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "depracer:UserToken" : "false"
        }
      }
    }
  ]
}
```



```

    "Bool" : {
      "depracer:MultiUser" : "true"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "depracer:GetAccountConfig",
      "depracer:GetTrack",
      "depracer:ListTracks",
      "depracer:TestRewardFunction"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "depracer:Admin*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerFullAccess

설명: 이 정책은 AWS DeepRacer에 대한 전체 액세스 권한을 제공합니다. 또한 관련 서비스(예: S3)에 대한 선택적 액세스를 제공합니다.

AWSDeepRacerFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 5일, 22:03 UTC
- 편집된 시간: 2020년 10월 5일, 22:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

```

    "s3:PutBucketPolicy",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:GetObjectAcl",
    "s3:GetBucketLocation"
  ],
  "Resource" : [
    "arn:aws:s3::*DeepRacer*",
    "arn:aws:s3::*Deepracer*",
    "arn:aws:s3::*deepracer*",
    "arn:aws:s3:::dr-*",
    "arn:aws:s3::*DeepRacer*/**",
    "arn:aws:s3::*Deepracer*/**",
    "arn:aws:s3::*deepracer*/**",
    "arn:aws:s3:::dr-*/**"
  ]
}
]
}
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerRoboMakerAccessPolicy

설명: 사용자 대신 필요한 리소스를 생성하고 AWS 서비스를 호출할 수 있습니다. RoboMaker

AWSDeepRacerRoboMakerAccessPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerRoboMakerAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 2월 28일, 21:59 UTC
- 편집된 시간: 2019년 2월 28일, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeepRacerServiceRolePolicy

설명: 사용자 대신 필요한 리소스를 생성하고 AWS 서비스를 호출할 수 있습니다. DeepRacer

AWSDeepRacerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 2월 28일, 21:58 UTC
- 편집된 시간: 2019년 6월 12일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDenyAll

설명: 모든 액세스를 거부합니다.

AWSDenyAll [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDenyAll를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 1일, 22:36 UTC
- 편집 시간: 2023년 12월 18일 16:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeviceFarmFullAccess

설명: 모든 AWS Device Farm 작업에 대한 전체 액세스 권한을 제공합니다.

AWSDeviceFarmFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeviceFarmFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 13일, 16:37 UTC
- 편집된 시간: 2015년 7월 13일, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeviceFarmServiceRolePolicy

설명: 사용자 대신 EC2 네트워크 API를 호출할 수 있는 권한을 AWS Device Farm에 부여하십시오.

AWSDeviceFarmServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 20일, 21:02 UTC
- 편집된 시간: 2022년 9월 20일, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDeviceFarmTestGridServiceRolePolicy

설명: 사용자 대신 EC2 API를 호출할 수 있는 권한을 AWS Device Farm에 부여하십시오.

AWSDeviceFarmTestGridServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 26일, 22:01 UTC
- 편집된 시간: 2021년 5월 26일, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDirectConnectFullAccess

설명: 를 통해 AWS Direct Connect에 대한 전체 액세스를 제공합니다 AWS Management Console.

AWSDirectConnectFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectConnectFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 4월 30일, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDirectConnectReadOnlyAccess

설명: 를 통해 AWS Direct Connect에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AWSDirectConnectReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectConnectReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 5월 18일, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ]
    }
  ]
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDirectConnectServiceRolePolicy

설명: 사용자를 대신하여 AWS 리소스를 만들고 관리할 수 있는 AWS Direct Connect 권한을 제공합니다.

AWSDirectConnectServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 14일, 18:35 UTC
- 편집된 시간: 2021년 1월 14일, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDirectoryServiceFullAccess

설명: AWS Directory Service에 대한 전체 액세스 권한을 제공합니다.

AWSDirectoryServiceFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectoryServiceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 4월 2일 20:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDirectoryServiceReadOnlyAccess

설명: AWS Directory Service에 대한 읽기 전용 액세스를 제공합니다.

AWSDirectoryServiceReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectoryServiceReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2018년 9월 25일, 21:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDiscoveryContinuousExportFirehosePolicy

설명: AWS Discovery Continuous Export에 필요한 AWS 리소스에 대한 쓰기 액세스 권한을 제공합니다.

AWSDiscoveryContinuousExportFirehosePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDiscoveryContinuousExportFirehosePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 8월 9일, 18:29 UTC
- 편집된 시간: 2021년 6월 8일, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDMSFleetAdvisorServiceRolePolicy

설명: DMS 플릿 어드바이저가 사용자를 대신하여 CloudWatch 지표를 관리할 수 있습니다.

AWSDMSFleetAdvisorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 6일, 09:10 UTC
- 편집된 시간: 2023년 3월 6일, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSDMSServerlessServiceRolePolicy

설명: 사용자 대신 계정에서 AWS DMS 리소스를 만들고 관리할 수 있는 DMS 서버리스 권한을 부여합니다.

AWSDMSServerlessServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 18일, 20:28 UTC
- 편집된 시간: 2023년 5월 18일, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEC2CapacityReservationFleetRolePolicy

설명: EC2 CapacityReservation 플릿 서비스가 용량 예약을 관리할 수 있도록 합니다.

AWSEC2CapacityReservationFleetRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 29일, 14:43 UTC
- 편집된 시간: 2021년 9월 29일, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEC2FleetServiceRolePolicy

설명: EC2 플릿에서 인스턴스를 시작하고 관리할 수 있습니다.

AWSEC2FleetServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 21일, 00:08 UTC
- 편집된 시간: 2020년 5월 4일, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEC2SpotFleetServiceRolePolicy

설명: EC2 스팟 플릿이 스팟 플릿 인스턴스를 시작하고 관리할 수 있도록 허용합니다.

AWSEC2SpotFleetServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 23일, 19:13 UTC
- 편집된 시간: 2020년 3월 16일, 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEC2SpotServiceRolePolicy

설명: EC2 스팟에서 스팟 인스턴스를 시작하고 관리할 수 있습니다.

AWSEC2SpotServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 18일, 18:51 UTC
- 편집된 시간: 2018년 12월 12일, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEC2VssSnapshotPolicy

설명: 이 정책은 Amazon EC2 Windows 인스턴스에 연결된 IAM 역할에 연결되어 있으며, 이를 통해 Amazon EC2 VSS 솔루션이 Amazon 머신 이미지 (AMI) 및 EBS 스냅샷에 태그를 생성하고 추가할 수 있습니다.

AWSEC2VssSnapshotPolicy 관리형 [AWS 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSEC2VssSnapshotPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 3월 27일 16:32 UTC
- 편집 시간: 2024년 3월 27일 16:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSECRPullThroughCache_ServiceRolePolicy

설명: AWS ECR 풀스루 캐시에서 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있습니다.

AWSECRPullThroughCache_ServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2021년 11월 26일, 21:51 UTC
- 편집된 시간: 2023년 11월 13일, 15:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

설명: 사용자 지정 플랫폼 빌더 환경의 인스턴스에 EC2 인스턴스를 시작하고, EBS 스냅샷과 AMI를 생성하고, 로그를 Amazon Logs로 스트리밍하고, Amazon CloudWatch S3에 아티팩트를 저장할 수 있는 권한을 제공합니다.

AWSElasticBeanstalkCustomPlatformforEC2Role [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkCustomPlatformforEC2Role를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 21일, 22:50 UTC
- 편집된 시간: 2017년 2월 21일, 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkEnhancedHealth

설명: 건강 AWS 모니터링 시스템을 위한 Elastic Beanstalk 서비스 정책

AWSElasticBeanstalkEnhancedHealth [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkEnhancedHealth를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 8일, 23:17 UTC
- 편집된 시간: 2018년 4월 9일, 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkMaintenance

설명: 유지 AWS 관리 목적으로 사용자를 대신하여 리소스를 업데이트할 수 있는 제한된 권한을 부여하는 Elastic Beanstalk 서비스 역할 정책입니다.

AWSElasticBeanstalkMaintenance [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 1월 11일, 23:22 UTC
- 편집 시간: 2024년 4월 29일 21:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

설명: 이 정책은 AWS Elastic Beanstalk 환경의 관리형 업데이트를 수행하는 데 사용되는 Elastic Beanstalk 서비스 역할을 위한 것입니다. 이 정책은 다른 사용자나 역할에 연결되어서는 안 됩니다. 이 정책은 EC2 AutoScaling, ECS, Elastic Load Balancing 등을 비롯한 다양한 AWS 서비스에서 리소스를 생성하고 관리할 수 있는 광범위한 권한을 부여합니다. CloudFormation 또한 이 정책은 해당 서비스에 사용할 수 있는 모든 IAM 역할의 전달을 허용합니다.

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 3일, 22:18 UTC
- 편집된 시간: 2023년 3월 23일, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

설명: AWS 관리형 업데이트에 제한된 권한을 부여하는 Elastic Beanstalk 서비스 역할 정책입니다.

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 21일, 22:35 UTC
- 편집 시간: 2024년 4월 29일 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkMulticontainerDocker

설명: Amazon EC2 Container Service를 사용하여 컨테이너 배포 작업을 관리할 수 있도록 멀티컨테이너 Docker 환경의 인스턴스에 액세스 권한을 제공하십시오.

AWSElasticBeanstalkMulticontainerDocker [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkMulticontainerDocker를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:15 UTC
- 편집된 시간: 2023년 3월 23일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkReadOnly

설명: 읽기 전용 권한을 부여합니다. 운영자가 Elastic AWS Beanstalk 애플리케이션과 관련된 리소스에 대한 정보를 검색하기 위해 직접 액세스할 수 있도록 명시적으로 허용합니다.

AWSElasticBeanstalkReadOnly [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 19:02 UTC
- 편집된 시간: 2021년 1월 22일, 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleCore

설명: AWSElasticBeanstalkRoleCore (Elastic Beanstalk 운영 역할) 웹 서비스 환경의 핵심 작업을 허용합니다.

AWSElasticBeanstalkRoleCore [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleCore를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:48 UTC
- 편집 시간: 2024년 4월 30일 00:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```

        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
    }
}
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReleaseAddress",
    "ec2:AllocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteSecurityGroup",
    "ec2:AuthorizeSecurityGroup*",
    "ec2:RevokeSecurityGroup*",
    "ec2:CreateLaunchTemplate*",
    "ec2>DeleteLaunchTemplate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LTRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:*LoadBalancer*",
    "autoscaling:*AutoScalingGroup",
    "autoscaling:*LaunchConfiguration",
    "autoscaling>DeleteScheduledAction",

```

```

    "autoscaling:DetachInstances",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:ResumeProcesses",
    "autoscaling:SuspendProcesses",
    "autoscaling:*Tags"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
  ]
},
{
  "Sid" : "ASGPolicy",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DeletePolicy"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EBSLR",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
    }
  }
},
{
  "Sid" : "S30bj",
  "Effect" : "Allow",
  "Action" : [

```

```
    "s3:Delete*",
    "s3:Get*",
    "s3:Put*"
  ],
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*/**",
    "arn:aws:s3:::elasticbeanstalk-env-resources-*/**"
  ]
},
{
  "Sid" : "S3Bucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucket*",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Sid" : "CFN",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation:ListStackResources",
    "cloudformation:UpdateStack",
    "cloudformation:ContinueUpdateRollback",
    "cloudformation:CancelUpdateStack",
    "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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleCWL

설명: (Elastic Beanstalk 운영 역할) Amazon Logs 로그 그룹을 관리할 CloudWatch 수 있는 환경을 허용합니다.

AWSElasticBeanstalkRoleCWL [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleCWL를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:49 UTC
- 편집된 시간: 2020년 6월 5일, 21:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleECS

설명: (Elastic Beanstalk 운영 역할) 다중 컨테이너 Docker 환경에서 Amazon ECS 클러스터를 관리할 수 있도록 합니다.

AWSElasticBeanstalkRoleECS [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleECS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:47 UTC
- 편집된 시간: 2023년 3월 23일, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleRDS

설명: (Elastic Beanstalk 운영 역할) Amazon RDS 인스턴스를 통합할 수 있는 환경을 허용합니다.

AWSElasticBeanstalkRoleRDS [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleRDS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:46 UTC
- 편집된 시간: 2020년 6월 5일, 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleSNS

설명: (Elastic Beanstalk 운영 역할) Amazon SNS 주제 통합을 지원하는 환경을 허용합니다.

AWSElasticBeanstalkRoleSNS [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleSNS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:46 UTC
- 편집된 시간: 2020년 6월 5일, 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkRoleWorkerTier

설명: (Elastic Beanstalk 운영 역할) 작업자 환경 계층이 Amazon DynamoDB 테이블과 Amazon SQS 대기열을 생성할 수 있도록 허용합니다.

AWSElasticBeanstalkRoleWorkerTier [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleWorkerTier를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:43 UTC
- 편집된 시간: 2020년 6월 5일, 21:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkService

설명: 이 정책은 지원 중단될 예정입니다. 지침은 설명서를 참조하십시오: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS 사용자를 대신하여 리소스 (AutoScaling예: EC2, CloudFormation S3, ELB 등) 를 생성하고 관리할 수 있는 권한을 부여하는 Elastic Beanstalk 서비스 역할 정책입니다.

AWSElasticBeanstalkService [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkService를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2016년 4월 11일, 20:27 UTC
- 편집된 시간: 2023년 5월 10일, 19:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkServiceRolePolicy

설명: AWS 사용자를 대신하여 리소스 (AutoScaling예: EC2, CloudFormation S3, ELB 등) 를 생성하고 관리할 수 있는 권한을 부여하는 Elastic Beanstalk 서비스 연결 역할 정책입니다.

AWSElasticBeanstalkServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 13일, 23:46 UTC
- 편집된 시간: 2019년 6월 6일, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkWebTier

설명: 웹 서버 환경의 인스턴스에 Amazon S3에 로그 파일을 업로드할 수 있는 액세스 권한을 제공하십시오.

AWSElasticBeanstalkWebTier [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkWebTier를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:08 UTC
- 편집된 시간: 2020년 9월 9일, 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticBeanstalkWorkerTier

설명: 작업자 환경의 인스턴스에 Amazon S3에 로그 파일을 업로드하고, Amazon SQS를 사용하여 애플리케이션의 작업 대기열을 모니터링하고, Amazon DynamoDB를 사용하여 리더 선출을 수행하고, Amazon에 상태 모니터링을 위한 지표를 게시할 수 있는 액세스 권한을 제공합니다. CloudWatch

AWSElasticBeanstalkWorkerTier [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkWorkerTier를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:12 UTC
- 편집된 시간: 2020년 9월 9일, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

설명: 이 정책은 AWS Elastic Disaster Recovery (DRS) 와 함께 외부 서버를 복구하는 데 사용되는 AWS 복제 에이전트를 설치할 수 있도록 AWS합니다. AWS 복제 에이전트의 설치 단계에서 자격 증명을 제공하는 IAM 사용자 또는 역할에 이 정책을 연결하십시오.

AWSElasticDisasterRecoveryAgentInstallationPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryAgentInstallationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:37 UTC
- 편집 시간: 2023년 11월 27일 12:38 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryAgentInstallationPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryAgentPolicy

설명: 이 정책은 AWS Elastic Disaster Recovery (DRS) 와 함께 소스 서버를 복구하는 데 사용되는 AWS 복제 에이전트를 사용할 수 있도록 AWS 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSElasticDisasterRecoveryAgentPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryAgentPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:32 UTC
- 편집 시간: 2023년 11월 27일 13:44 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWS Elastic Disaster Recovery Console Full Access

설명: 이 정책은 AWS 탄력적 재해 복구 (DRS) 의 모든 퍼블릭 API에 대한 전체 액세스 권한과 KMS 키, 라이선스 관리자, 리소스 그룹, Elastic Load Balancing, IAM 및 EC2 정보를 읽을 수 있는 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWS Elastic Disaster Recovery Console Full Access [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWS Elastic Disaster Recovery Console Full Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:46 UTC
- 편집된 시간: 2023년 10월 16일, 12:24 UTC

- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

설명: 이 정책은 DRS (AWS Elastic Disaster Recovery) 의 모든 퍼블릭 API와 AWS DRS 콘솔에서 사용하는 다른 AWS 서비스의 모든 퍼블릭 API에 대한 전체 액세스를 제공합니다. AWS 이 정책을 사용자 또는 역할에 연결하십시오.

AWSElasticDisasterRecoveryConsoleFullAccess_v2 [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryConsoleFullAccess_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 27일 13:35 UTC
- 편집 시간: 2024년 5월 19일 07:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
{
  "Sid" : "ConsoleFullAccess1",
  "Effect" : "Allow",
  "Action" : [
    "drs:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess2",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
```

```
    "Sid" : "ConsoleFullAccess4",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups:ListGroups",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess6",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess7",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess8",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryConversionServerPolicy

설명: 이 정책은 AWS Elastic 재해 복구 변환 서버의 인스턴스 역할에 연결됩니다. 이 정책은 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Conversion Servers가 DRS 서비스와 통신할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 DRS에 의해 (EC2 Instance Profile로) DRS Conversion Servers에 연결되며, 필요할 때 DRS에 의해 자동으로 시작되고 종료됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다. DRS Conversion Servers는 사용자가 DRS 콘솔, CLI 또는 API를 사용하여 소스 서버를 복구하도록 선택할 때 Elastic Disaster Recovery에서 사용됩니다.

AWSElasticDisasterRecoveryConversionServerPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryConversionServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 13:42 UTC
- 편집 시간: 2023년 11월 27일 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

설명: 이 정책을 통해 AWS Elastic Disaster Recovery (DRS) 는 계정 간 복제 및 계정 간 장애 복구를 지원할 수 있습니다.

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryCrossAccountReplicationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 5월 14일, 07:16 UTC
- 편집 시간: 2024년 1월 17일 13:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

설명: 이 정책은 AWS Elastic Disaster Recovery (DRS) 에서 EC2에서 실행되는 소스 서버 (지역 간 또는 AZ 간) 를 복구하는 데 사용하는 AWS 복제 에이전트의 설치 및 사용을 허용합니다. 이 정책이 있는 IAM 역할은 EC2 Instances에 (EC2 Instance Profile로) 연결되어야 합니다.

AWSElasticDisasterRecoveryEc2InstancePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryEc2InstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 5월 26일, 12:30 UTC
- 편집 시간: 2023년 11월 27일 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

설명: AWSElasticDisasterRecoveryFailbackInstallationPolicy 정책을 IAM ID에 연결할 수 있습니다. 이 정책을 사용하면 Recovery Instances를 원래 소스 인프라로 페일백하는 데 사용되는 Elastic Disaster Recovery Failback Client를 설치할 수 있습니다. Elastic Disaster Recovery Failback Client를 실행할 때 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 이 정책을 연결하세요.

AWSElasticDisasterRecoveryFailbackInstallationPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryFailbackInstallationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 11:02 UTC
- 편집 시간: 2023년 11월 27일 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryFailbackPolicy

설명: 이 정책은 복구 인스턴스를 원래 소스 인프라로 페일백하는 데 사용되는 Elastic Disaster Recovery Failback 클라이언트를 사용할 수 있도록 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSElasticDisasterRecoveryFailbackPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryFailbackPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:41 UTC
- 편집 시간: 2023년 11월 27일 12:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

설명: 이 정책을 사용하면 Amazon SSM 및 추가 서비스 필수 권한을 사용하여 AWS 탄력적 재해 복구 (AWS DR) 에서 출시 후 작업을 실행할 수 있습니다. 이 정책을 IAM 역할 또는 사용자에게 연결하세요.

AWSElasticDisasterRecoveryLaunchActionsPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryLaunchActionsPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 13일, 07:38 UTC
- 편집 시간: 2024년 5월 19일 07:29 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryLaunchActionsPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "drs.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "LaunchActionsPolicy2",
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "drs.amazonaws.com"
            ]
        },
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "LaunchActionsPolicy3",
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*",
        "arn:aws:ssm:*:*:document/AWSCodeDeployAgent-*",

```

```
"arn:aws:ssm:*::document/AWSConfigRemediation-*",
"arn:aws:ssm:*::document/AWSConformancePacks-*",
"arn:aws:ssm:*::document/AWSDisasterRecovery-*",
"arn:aws:ssm:*::document/AWSDistro0Tel-*",
"arn:aws:ssm:*::document/AWSDocs-*",
"arn:aws:ssm:*::document/AWSEC2-*",
"arn:aws:ssm:*::document/AWSEC2Launch-*",
"arn:aws:ssm:*::document/AWSFIS-*",
"arn:aws:ssm:*::document/AWSFleetManager-*",
"arn:aws:ssm:*::document/AWSIncidents-*",
"arn:aws:ssm:*::document/AWSKinesisTap-*",
"arn:aws:ssm:*::document/AWSMigration-*",
"arn:aws:ssm:*::document/AWSNVMe-*",
"arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
"arn:aws:ssm:*::document/AWSObservabilityExporter-*",
"arn:aws:ssm:*::document/AWSPVDriver-*",
"arn:aws:ssm:*::document/AWSQuickSetupType-*",
"arn:aws:ssm:*::document/AWSQuickStarts-*",
"arn:aws:ssm:*::document/AWSRefactorSpaces-*",
"arn:aws:ssm:*::document/AWSResilienceHub-*",
"arn:aws:ssm:*::document/AWSSAP-*",
"arn:aws:ssm:*::document/AWSSAPTools-*",
"arn:aws:ssm:*::document/AWSSQLServer-*",
"arn:aws:ssm:*::document/AWSSSO-*",
"arn:aws:ssm:*::document/AWSSupport-*",
"arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
"arn:aws:ssm:*::document/AmazonCloudWatch-*",
"arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
"arn:aws:ssm:*::document/AmazonECS-*",
"arn:aws:ssm:*::document/AmazonEFSUtils-*",
"arn:aws:ssm:*::document/AmazonEKS-*",
"arn:aws:ssm:*::document/AmazonInspector-*",
"arn:aws:ssm:*::document/AmazonInspector2-*",
"arn:aws:ssm:*::document/AmazonInternal-*",
"arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
"arn:aws:ssm:*::document/AwsVssComponents-*",
"arn:aws:ssm:*::automation-definition/AWS-*:*",
"arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
"arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
"arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
"arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
"arn:aws:ssm:*::automation-definition/AWSDistro0Tel-*:*",
"arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
"arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
```

```

    "arn:aws:ssm::*:automation-definition/AWSEC2Launch-*:*",
    "arn:aws:ssm::*:automation-definition/AWSFIS-*:*",
    "arn:aws:ssm::*:automation-definition/AWSFleetManager-*:*",
    "arn:aws:ssm::*:automation-definition/AWSIncidents-*:*",
    "arn:aws:ssm::*:automation-definition/AWSKinesisTap-*:*",
    "arn:aws:ssm::*:automation-definition/AWSMigration-*:*",
    "arn:aws:ssm::*:automation-definition/AWSNVMe-*:*",
    "arn:aws:ssm::*:automation-definition/AWSNitroEnclavesWindows-*:*",
    "arn:aws:ssm::*:automation-definition/AWSObservabilityExporter-*:*",
    "arn:aws:ssm::*:automation-definition/AWSPVDriver-*:*",
    "arn:aws:ssm::*:automation-definition/AWSQuickSetupType-*:*",
    "arn:aws:ssm::*:automation-definition/AWSQuickStarts-*:*",
    "arn:aws:ssm::*:automation-definition/AWSRefactorSpaces-*:*",
    "arn:aws:ssm::*:automation-definition/AWSResilienceHub-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSAP-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSAPTools-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSQLServer-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSSO-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSupport-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSystemsManagerSAP-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonCloudWatch-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonCloudWatchAgent-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonECS-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonEFSUtils-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonEKS-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInspector-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInspector2-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInternal-*:*",
    "arn:aws:ssm::*:automation-definition/AwsEnaNetworkDriver-*:*",
    "arn:aws:ssm::*:automation-definition/AwsVssComponents-*:*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "LaunchActionsPolicy4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      },
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy5",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy6",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListDocuments",
      "ssm:ListCommandInvocations"
    ],
    "Resource" : "*"
  },
},
```

```
{
  "Sid" : "LaunchActionsPolicy7",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListDocumentVersions",
    "ssm:GetDocument",
    "ssm:DescribeDocument"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/*"
},
{
  "Sid" : "LaunchActionsPolicy8",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "LaunchActionsPolicy9",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecoveryService-*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "ssm.amazonaws.com"
    }
  }
},
{
  "Sid" : "LaunchActionsPolicy10",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter",
    "ssm:PutParameter"
  ],
}
```

```

    "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy11",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "drs.amazonaws.com"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

설명: 이 정책을 통해 AWS 탄력적 재해 복구 (DRS) 는 네트워크 복제를 지원할 수 있습니다.

AWSElasticDisasterRecoveryNetworkReplicationPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryNetworkReplicationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 11일, 12:36 UTC
- 편집 시간: 2024년 1월 2일 13:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryReadOnlyAccess

설명: AWSElasticDisasterRecoveryReadOnlyAccess 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 DRS 콘솔을 완전히 읽기 전용으로 사용하기 위해 필요한 다른 AWS 서비스의 일부 읽기 전용 API뿐만 아니라 Elastic Disaster Recovery (DRS)의 모든 읽기 전용 퍼블릭 API에 대한 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

AWSElasticDisasterRecoveryReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:50 UTC
- 편집 시간: 2023년 11월 27일 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

설명: 이 정책은 Elastic Disaster Recovery의 복구 인스턴스의 인스턴스 역할에 연결됩니다. 이 정책을 사용하면 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Recovery Instance가 DRS 서비스와 통신하고 원래 소스 인프라로 페일백할 수 있습니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery를 통해 (EC2 Instance Profile로) DRS Recovery Instances에 연결됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSElasticDisasterRecoveryRecoveryInstancePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryRecoveryInstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:20 UTC
- 편집 시간: 2023년 11월 27일 13:11 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

설명: 이 정책은 Elastic 재해 복구 복제 서버의 인스턴스 역할에 연결됩니다. 이 정책은 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Replication Servers가 DRS 서비스와 통신하고 AWS 계정에 EBS 스냅샷을 생성할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery에 의해 필요에 따라 DRS에 의해 자동으로 시작 및 종료되는 DRS Replication Servers에 (EC2 Instance Profile로) 연결됩니다. DRS 복제 서버는 DRS에서 관리하는 복구 프로세스의 일환으로 외부 서버에서 외부 서버로의 AWS데이터 복제를 용이하게 하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSElasticDisasterRecoveryReplicationServerPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryReplicationServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 13:34 UTC
- 편집 시간: 2023년 11월 27일 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryServiceRolePolicy

설명: 이 정책은 Elastic Disaster Recovery가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AWSElasticDisasterRecoveryServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 10:56 UTC
- 편집 시간: 2024년 1월 17일 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    }
  ]
}
```

```
"Sid" : "DRSServiceRolePolicy6",
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeImages",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceTypes",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceState",
  "ec2:DescribeLaunchTemplateVersions",
  "ec2:DescribeLaunchTemplates",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSnapshots",
  "ec2:DescribeSubnets",
  "ec2:DescribeVolumes",
  "ec2:DescribeVolumeAttribute",
  "ec2:GetEbsDefaultKmsKeyId",
  "ec2:GetEbsEncryptionByDefault",
  "ec2:DescribeVpcAttribute",
  "ec2:DescribeInternetGateways",
  "ec2:DescribeVpcs",
  "ec2:DescribeNetworkAcls",
  "ec2:DescribeRouteTables",
  "ec2:DescribeDhcpOptions",
  "ec2:DescribeManagedPrefixLists",
  "ec2:GetManagedPrefixListEntries",
  "ec2:GetManagedPrefixListAssociations"
],
"Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeregisterImage"
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy11",
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteVolume",
      "ec2:ModifyVolume"
    ]
  }
],
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
},
{
  "Sid" : "DRSServiceRolePolicy12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy14",
  "Effect" : "Allow",
  "Action" : [
```



```
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy15",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy16",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "DRSServiceRolePolicy17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
```

```
"Sid" : "DRSServiceRolePolicy18",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateSnapshot"
],
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
}
},
{
  "Sid" : "DRSServiceRolePolicy19",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateSnapshot"
],
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
}
},
{
  "Sid" : "DRSServiceRolePolicy20",
"Effect" : "Allow",
"Action" : [
  "ec2:DetachVolume",
  "ec2:AttachVolume"
],
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
}
},
{
  "Sid" : "DRSServiceRolePolicy21",
"Effect" : "Allow",
"Action" : [
  "ec2:AttachVolume"
```

```
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy22",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*"
  },
  {
    "Sid" : "DRSServiceRolePolicy23",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy24",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ]
  }
],
```

```
{
  "Sid" : "DRSServiceRolePolicy25",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
    "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
    "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy26",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2::*:launch-template/*",
    "arn:aws:ec2::*:security-group/*",
    "arn:aws:ec2::*:volume/*",
    "arn:aws:ec2::*:snapshot/*",
    "arn:aws:ec2::*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate",
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy27",
  "Effect" : "Allow",
```

```

    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy28",
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

설명: 이 정책은 원본 서버 및 작업과 같은 DRS (AWS Elastic Disaster Recovery) 리소스에 대한 읽기 전용 액세스를 허용합니다. 또한 변환된 스냅샷을 생성하고 해당 EBS 스냅샷을 특정 계정과 공유할 수 있도록 허용합니다.

AWSElasticDisasterRecoveryStagingAccountPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryStagingAccountPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2022년 5월 26일, 09:49 UTC
- 편집 시간: 2023년 11월 27일, 13:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

설명: 이 정책은 AWS Elastic Disaster Recovery (DRS) 에서 소스 서버를 별도의 대상 계정으로 복구하고 파일백을 허용하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryStagingAccountPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 1월 5일, 12:11 UTC
- 편집 시간: 2023년 11월 27일 13:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ],
  {
```



```

    "Sid" : "DRSStagingAccountPolicyv23",
    "Effect" : "Allow",
    "Action" : "drs:IssueAgentCertificateForDrs",
    "Resource" : [
      "arn:aws:drs:*:*:source-server/*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

설명: AWS Elastic Load Balancing 컨트롤 플레인에 대한 서비스 연결 역할 정책 - 클래식

AWSElasticLoadBalancingClassicServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 19일, 22:36 UTC
- 편집된 시간: 2019년 10월 7일, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElasticLoadBalancingServiceRolePolicy

설명: AWS Elastic Load Balancing 컨트롤 플레인에 대한 서비스 연결 역할 정책

AWSElasticLoadBalancingServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 19일, 22:19 UTC
- 편집된 시간: 2021년 8월 26일, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaConvertFullAccess

설명: AWS Management Console 및 SDK를 MediaConvert 통해 AWS Elemental에 대한 전체 액세스 권한을 제공합니다.

AWSElementalMediaConvertFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaConvertFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 25일, 19:25 UTC
- 편집된 시간: 2019년 6월 10일, 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaConvertReadOnly

설명: AWS Management Console 및 SDK를 MediaConvert 통해 AWS Elemental에 대한 읽기 전용 액세스를 제공합니다.

AWSElementalMediaConvertReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaConvertReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 25일, 19:25 UTC
- 편집된 시간: 2019년 6월 10일, 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaLiveFullAccess

설명: AWS Elemental MediaLive 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSElementalMediaLiveFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaLiveFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 8일, 17:07 UTC
- 편집된 시간: 2020년 7월 8일, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```
"Effect" : "Allow",
"Action" : "medialive:*",
"Resource" : "*"
}
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaLiveReadOnly

설명: AWS Elemental MediaLive 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSElementalMediaLiveReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaLiveReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 8일, 16:38 UTC
- 편집된 시간: 2020년 7월 8일, 16:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaPackageFullAccess

설명: AWS Elemental MediaPackage 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSElementalMediaPackageFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaPackageFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 29일, 23:39 UTC
- 편집된 시간: 2017년 12월 29일, 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaPackageReadOnly

설명: AWS Elemental MediaPackage 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSElementalMediaPackageReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaPackageReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 12월 30일, 00:04 UTC
- 편집된 시간: 2017년 12월 30일, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaPackageV2FullAccess

설명: AWS Elemental MediaPackage V2 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSElementalMediaPackageV2FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaPackageV2FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 20:29 UTC
- 편집된 시간: 2023년 7월 25일, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaPackageV2ReadOnly

설명: AWS Elemental MediaPackage V2 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSElementalMediaPackageV2ReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaPackageV2ReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 20:31 UTC
- 편집된 시간: 2023년 7월 25일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaStoreFullAccess

설명: 모든 MediaStore API에 대한 전체 읽기 및 쓰기 액세스 권한을 제공합니다.

AWSElementalMediaStoreFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaStoreFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 5일, 23:15 UTC
- 편집된 시간: 2018년 3월 5일, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
{
  "Action" : [
    "mediastore:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "aws:SecureTransport" : "true"
    }
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaStoreReadOnly

설명: API에 MediaStore 대한 읽기 전용 권한을 제공합니다.

AWSElementalMediaStoreReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaStoreReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 8일, 19:48 UTC
- 편집된 시간: 2018년 3월 8일, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaTailorFullAccess

설명: AWS Elemental MediaTailor 리소스에 대한 전체 액세스 권한을 제공합니다.

AWSElementalMediaTailorFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaTailorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 23일, 00:04 UTC
- 편집된 시간: 2021년 11월 23일, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSElementalMediaTailorReadOnly

설명: AWS Elemental MediaTailor 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSElementalMediaTailorReadOnly [AWS 관리형 정책입니다](#).

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaTailorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 23일, 00:05 UTC
- 편집된 시간: 2021년 11월 23일, 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEnhancedClassicNetworkingMangementPolicy

설명: 향상된 클래식 네트워킹 관리 기능을 활성화하기 위한 정책입니다.

AWSEnhancedClassicNetworkingMangementPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 20일, 17:29 UTC
- 편집된 시간: 2017년 9월 20일, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEntityResolutionConsoleFullAccess

설명: AWS 엔티티 레졸루션 및 관련 서비스에 대한 콘솔 전체 액세스 권한을 제공합니다.

AWSEntityResolutionConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSEntityResolutionConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 17일, 17:54 UTC
- 편집된 시간: 2023년 10월 16일, 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSEntityResolutionConsoleReadOnlyAccess

설명: 를 통해 AWS 엔티티 해상도에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

AWSEntityResolutionConsoleReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSEntityResolutionConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 17일, 18:18 UTC
- 편집된 시간: 2023년 8월 17일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorEC2Access

설명: 이 정책은 EC2의 장애 주입 시뮬레이터 서비스 및 FIS 작업을 수행하는 데 필요한 기타 서비스에 권한을 부여합니다.

AWSFaultInjectionSimulatorEC2Access [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorEC2Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:39 UTC
- 편집 시간: 2023년 11월 27일 15:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorECSAccess

설명: 이 정책은 ECS의 장애 주입 시뮬레이터 서비스 및 FIS 작업을 수행하는 데 필요한 기타 서비스에 권한을 부여합니다.

AWSFaultInjectionSimulatorECSAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorECSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:37 UTC
- 편집 시간: 2024년 1월 25일 16:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorEKSAccess

설명: 이 정책은 EKS의 장애 주입 시뮬레이터 서비스 권한 및 FIS 작업을 수행하는 데 필요한 기타 서비스를 부여합니다.

AWSFaultInjectionSimulatorEKSAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorEKSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:34 UTC
- 편집된 시간: 2023년 11월 13일, 16:44 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorNetworkAccess

설명: 이 정책은 FIS 작업을 수행하는 데 필요한 EC2 네트워킹 및 기타 필수 서비스의 장애 주입 시뮬레이터 서비스 권한을 부여합니다.

AWSFaultInjectionSimulatorNetworkAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorNetworkAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:32 UTC
- 편집 시간: 2024년 1월 25일 16:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorRDSAccess

설명: 이 정책은 RDS의 장애 주입 시뮬레이터 서비스 권한 및 FIS 작업을 수행하는 데 필요한 기타 서비스를 부여합니다.

AWSFaultInjectionSimulatorRDSAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorRDSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:30 UTC
- 편집된 시간: 2023년 11월 13일, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFaultInjectionSimulatorSSMAccess

설명: 이 정책은 SSM의 장애 주입 시뮬레이터 서비스 권한 및 FIS 작업을 수행하는 데 필요한 기타 서비스를 부여합니다.

AWSFaultInjectionSimulatorSSMAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorSSMAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 15:33 UTC
- 편집된 시간: 2023년 6월 2일, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFinSpaceServiceRolePolicy

설명: Amazon에서 사용하거나 관리하는 리소스 AWS 서비스 및 액세스를 활성화하는 정책 FinSpace AWSFinSpaceServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 12일, 16:42 UTC
- 편집 시간: 2023년 12월 1일, 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFMAdminFullAccess

설명: AWS FM 관리자를 위한 전체 권한

AWSFMAdminFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFMAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 18:06 UTC
- 편집된 시간: 2022년 10월 20일, 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    ]
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFMAdminReadOnlyAccess

설명: FM 작업을 AWS 모니터링할 수 있는 AWS FM 관리자를 위한 읽기 전용 액세스

AWSFMAdminReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFMAdminReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 20:07 UTC
- 편집된 시간: 2022년 10월 31일, 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSFMMemberReadOnlyAccess

설명: AWS Firewall Manager 구성원 계정의 AWS WAF 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSFMMemberReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSFMMemberReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 21:05 UTC
- 편집된 시간: 2018년 5월 9일, 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSForWordPressPluginPolicy

설명: For 워드프레스 플러그인에 AWS 대한 관리형 정책

AWSForWordPressPluginPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSForWordPressPluginPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 30일, 00:27 UTC
- 편집된 시간: 2020년 1월 20일, 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGitSyncServiceRolePolicy

설명: AWS 코드 연결이 git 저장소의 콘텐츠를 동기화할 수 있도록 허용하는 정책

AWSGitSyncServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 16일, 17:05 UTC
- 편집 시간: 2024년 4월 26일 18:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlobalAcceleratorSLRPolicy

설명: AWS 글로벌 액셀러레이터에 EC2 엘라스틱 네트워크 인터페이스 및 보안 그룹을 관리할 수 있는 권한을 부여하는 정책.

AWSGlobalAcceleratorSLRPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 4월 5일, 19:39 UTC
- 편집된 시간: 2023년 9월 12일, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueConsoleFullAccess

설명: Glue를 통해 AWS Glue에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

AWSGlueConsoleFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 7월 14일, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueConsoleSageMakerNotebookFullAccess

설명: sagemaker 노트북 인스턴스를 통해 AWS Glue에 대한 전체 액세스 AWS Management Console 및 액세스 권한을 제공합니다.

AWSGlueConsoleSageMakerNotebookFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueConsoleSageMakerNotebookFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 5일, 17:52 UTC
- 편집된 시간: 2021년 7월 15일, 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AwsGlueDataBrewFullAccessPolicy

설명: DataBrew 를 통해 AWS Glue에 대한 전체 액세스 권한을 제공합니다 AWS Management Console. 또한 관련 서비스(예: S3, KMS, Glue)에 대한 선택적 액세스를 제공합니다.

AwsGlueDataBrewFullAccessPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueDataBrewFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 11일, 16:51 UTC
- 편집된 시간: 2022년 2월 4일, 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueDataBrewServiceRole

설명: 이 정책은 사용자의 글루 데이터 카탈로그에서 작업을 수행할 수 있는 권한을 부여합니다. 이 정책은 또한 ec2 작업에 대한 권한을 제공하여 Glue가 ENI를 생성하여 VPC의 리소스에 연결할 수 있도록 허용하고, lukeformation의 등록된 데이터에 액세스할 수 있도록 허용하고, 사용자의 cloudwatch에 액세스할 수 있는 권한을 부여합니다.

AWSGlueDataBrewServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueDataBrewServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 4일, 21:26 UTC
- 편집 시간: 2024년 3월 20일 23:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityType",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",

```

```
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::databrew-public-datasets-*"
  ]
},
{
  "Sid" : "EC2NetworkingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteNetworkInterface",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws-glue-service-resource" : "*"
    }
  },
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2GlueTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
```

```
        "aws:TagKeys" : [
            "aws-glue-service-resource"
        ]
    },
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
    ],
    {
        "Sid" : "GlueDatabrewLogGroupPermissions",
        "Effect" : "Allow",
        "Action" : [
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents"
        ],
        "Resource" : [
            "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
        ]
    },
    {
        "Sid" : "LakeFormationPermissions",
        "Effect" : "Allow",
        "Action" : [
            "lakeformation:GetDataAccess"
        ],
        "Resource" : "*"
    },
    {
        "Sid" : "SecretsManagerPermissions",
        "Effect" : "Allow",
        "Action" : [
            "secretsmanager:GetSecretValue"
        ],
        "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueSchemaRegistryFullAccess

설명: AWS Glue 스키마 레지스트리 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSGlueSchemaRegistryFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueSchemaRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 00:19 UTC
- 편집된 시간: 2020년 11월 20일, 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueSchemaRegistryReadOnlyAccess

설명: AWS Glue 스키마 레지스트리 서비스에 대한 읽기 전용 액세스를 제공합니다.

AWSGlueSchemaRegistryReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueSchemaRegistryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 00:20 UTC
- 편집된 시간: 2020년 11월 20일, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueServiceNotebookRole

설명: 고객이 노트북 서버를 관리할 수 있는 AWS Glue 서비스 역할 정책

AWSGlueServiceNotebookRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueServiceNotebookRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 10월 9일, 15:59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGlueServiceRole

설명: EC2, S3, Cloudwatch 로그를 비롯한 관련 서비스에 대한 액세스를 허용하는 AWS Glue 서비스 역할 정책

AWSGlueServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 9월 11일, 16:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AwsGlueSessionUserRestrictedNotebookPolicy

설명: 사용자가 해당 사용자와 관련된 노트북 세션만 만들고 사용할 수 있는 권한을 제공합니다. 이 정책에는 제한된 Glue 세션 역할을 사용자가 전달할 수 있도록 명시적으로 허용하는 권한도 포함되어 있습니다.

AwsGlueSessionUserRestrictedNotebookPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedNotebookPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 18일, 15:24 UTC
- 편집 시간: 2023년 11월 22일 01:32 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

설명: 세션을 제외한 모든 AWS Glue 리소스에 대한 전체 액세스 권한을 제공합니다. 사용자가 자신과 연결된 노트북 세션만 생성하고 사용할 수 있도록 허용합니다. 이 정책에는 Glue가 다른 AWS 서비스의 AWS Glue 리소스를 관리하는 데 필요한 기타 권한도 포함됩니다.

AwsGlueSessionUserRestrictedNotebookServiceRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedNotebookServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 18일, 15:27 UTC
- 편집된 시간: 2022년 4월 18일, 15:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AwsGlueSessionUserRestrictedPolicy

설명: 사용자가 해당 사용자와 연결된 대화형 세션만 만들고 사용할 수 있는 권한을 제공합니다. 이 정책에는 제한된 Glue 세션 역할을 사용자가 전달할 수 있도록 명시적으로 허용하는 권한도 포함되어 있습니다.

AwsGlueSessionUserRestrictedPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 14일, 21:31 UTC
- 편집 시간: 2024년 4월 29일 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ]
    }
  ]
}
```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/owner" : "${aws:userid}"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    }
  },
  {
    "Sid" : "AllowCompletionActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:StartCompletion",
      "glue:GetCompletion"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:completion/*"
    ]
  },
  {
    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:RunStatement",
      "glue:GetStatement",
      "glue:ListStatements",
      "glue:CancelStatement",
      "glue:StopSession",
      "glue>DeleteSession",
      "glue:GetSession"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/owner" : "${aws:userid}"
      }
    }
  }
},
```

```
{
  "Sid" : "AllowListSessions",
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DenyTagActions",
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Sid" : "AllowPassRoleActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
```

```
    }
  }
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AwsGlueSessionUserRestrictedServiceRole

설명: 세션을 제외한 모든 AWS Glue 리소스에 대한 전체 액세스 권한을 제공합니다. 사용자와 연결된 대화형 세션만 사용자가 생성하고 사용할 수 있도록 허용합니다. 이 정책에는 Glue가 다른 AWS 서비스의 AWS Glue 리소스를 관리하는 데 필요한 기타 권한도 포함됩니다.

AwsGlueSessionUserRestrictedServiceRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 14일, 21:30 UTC
- 편집 시간: 2024년 4월 29일 22:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

```
    ]  
  }  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGrafanaAccountAdministrator

설명: Amazon Grafana 내에서 전체 조직을 위한 작업 공간을 생성하고 관리할 수 있는 액세스를 제공합니다.

AWSGrafanaAccountAdministrator [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGrafanaAccountAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:20 UTC
- 편집된 시간: 2022년 2월 15일, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGrafanaConsoleReadOnlyAccess

설명: Amazon Grafana에서 읽기 전용 작업에 액세스할 수 있습니다.

AWSGrafanaConsoleReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGrafanaConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:10 UTC
- 편집된 시간: 2022년 2월 15일, 22:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGrafanaWorkspacePermissionManagement

설명: AWS Grafana 작업 영역에 대한 사용자 및 그룹 권한을 업데이트하는 기능만 제공합니다.

AWSGrafanaWorkspacePermissionManagement [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGrafanaWorkspacePermissionManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:15 UTC
- 편집된 시간: 2023년 3월 15일, 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGrafanaWorkspacePermissionManagementV2

설명: Amazon 관리형 Grafana 작업 영역에 대한 IAM ID 센터 (IdC) 사용자 및 그룹 권한을 업데이트하는 기능을 제공합니다.

AWSGrafanaWorkspacePermissionManagementV2 [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSGrafanaWorkspacePermissionManagementV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 1월 5일 18:39 UTC
- 편집 시간: 2024년 1월 5일 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGreengrassFullAccess

설명: 이 정책은 AWS Greengrass 구성, 관리 및 배포 작업에 대한 전체 액세스 권한을 부여합니다.

AWSGreengrassFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGreengrassFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 5월 3일, 00:47 UTC
- 편집된 시간: 2017년 5월 3일, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGreengrassReadOnlyAccess

설명: 이 정책은 AWS Greengrass 구성, 관리 및 배포 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSGreengrassReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGreengrassReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 30일, 16:01 UTC
- 편집된 시간: 2018년 10월 30일, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGreengrassResourceAccessRolePolicy

설명: Lambda AWS 및 IoT 사물 새도우를 비롯한 관련 서비스에 대한 액세스를 허용하는 AWS Greengrass 서비스 역할에 대한 정책입니다. AWS

AWSGreengrassResourceAccessRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSGreengrassResourceAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 2월 14일, 21:17 UTC
- 편집된 시간: 2018년 11월 14일, 00:35 UTC

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

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSGroundStationAgentInstancePolicy

설명: AWS Ground Station 에이전트를 사용할 수 있는 Dataflow 엔드포인트 인스턴스 권한을 제공합니다.

AWSGroundStationAgentInstancePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGroundStationAgentInstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 29일, 15:23 UTC
- 편집된 시간: 2023년 3월 29일, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSHealth_EventProcessorServiceRolePolicy

설명: AWS Health에서 Health 이벤트 프로세서 기능을 활성화할 수 있도록 허용합니다.

AWSHealth_EventProcessorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 13일, 19:24 UTC
- 편집된 시간: 2023년 1월 13일, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSHealthFullAccess

설명: AWS Health API, 알림 및 Personal Health 대시보드에 대한 전체 액세스를 허용합니다.

AWSHealthFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSHealthFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 6일, 12:30 UTC
- 편집된 시간: 2020년 11월 16일, 18:11 UTC

- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSHealthImagingFullAccess

설명: AWS 건강 영상 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSHealthImagingFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSHealthImagingFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 23:39 UTC
- 편집된 시간: 2023년 7월 25일, 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSHealthImagingReadOnlyAccess

설명: AWS Health Imaging 서비스에 대한 읽기 전용 액세스를 제공합니다.

AWSHealthImagingReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSHealthImagingReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 23:40 UTC
- 편집된 시간: 2023년 8월 1일, 15:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIAMIdentityCenterAllowListForIdentityContext

설명: IAM Identity Center 자격 증명 컨텍스트에서 맡는 역할에 허용되는 작업 목록을 제공합니다. AWS 보안 토큰 서비스 (AWS STS) 는 이 정책을 수임된 역할에 자동으로 연결합니다. ID 컨텍스트는 ProvidedContext로 전달됩니다.

AWSIAMIdentityCenterAllowListForIdentityContext [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIAMIdentityCenterAllowListForIdentityContext를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 8일, 15:21 UTC
- 편집 시간: 2024년 5월 16일 22:01 UTC
- ARN: arn:aws:iam::aws:policy/
AWSIAMIdentityCenterAllowListForIdentityContext

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIdentitySyncFullAccess

설명: ID 동기화 서비스에 대한 전체 액세스 권한을 부여합니다.

AWSIdentitySyncFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIdentitySyncFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 3월 23일, 23:29 UTC
- 편집된 시간: 2022년 3월 23일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIdentitySyncReadOnlyAccess

설명: ID 동기화 서비스에 대한 읽기 전용 액세스

AWSIdentitySyncReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIdentitySyncReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 3월 23일, 23:29 UTC
- 편집된 시간: 2022년 3월 23일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSImageBuilderFullAccess

설명: 모든 AWS Image Builder 작업에 대한 전체 액세스 권한과 관련 AWS 서비스에 대한 리소스 범위 지정 액세스를 제공합니다.

AWSImageBuilderFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSImageBuilderFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 20일, 18:25 UTC
- 편집된 시간: 2021년 4월 13일, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSImageBuilderReadOnlyAccess

설명: 모든 AWS Image Builder 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSImageBuilderReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSImageBuilderReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 19일, 22:29 UTC
- 편집된 시간: 2019년 12월 19일, 22:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSImportExportFullAccess

설명: 에서 생성된 작업에 대한 읽기 및 쓰기 액세스 권한을 제공합니다 AWS 계정.

AWSImportExportFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSImportExportFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSImportExportReadOnlyAccess

설명: 에서 생성된 작업에 대한 읽기 전용 액세스를 제공합니다 AWS 계정.

AWSImportExportReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSImportExportReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "Effect" : "Allow",
    "Action" : [
      "importexport:ListJobs",
      "importexport:GetStatus"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

설명: 인시던트 관리자에게 인시던트 관리의 일환으로 다른 AWS 서비스를 호출할 수 있는 권한을 부여합니다.

AWSIncidentManagerIncidentAccessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIncidentManagerIncidentAccessServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 13일, 00:01 UTC
- 편집 시간: 2024년 2월 20일 23:02 UTC
- ARN: arn:aws:iam::aws:policy/
AWSIncidentManagerIncidentAccessServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIncidentManagerResolverAccess

설명: 이 정책은 사용자 지정 타임라인 이벤트 및 관련 항목에 대한 전체 액세스 권한과 함께 인시던트를 시작, 조회, 업데이트할 수 있는 권한을 부여합니다. 인시던트를 생성하고 해결할 사용자에게 이 정책을 할당하세요.

AWSIncidentManagerResolverAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIncidentManagerResolverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 10일, 06:12 UTC
- 편집된 시간: 2021년 5월 10일, 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIncidentManagerServiceRolePolicy

설명: 이 정책은 인시던트 관리자에게 사용자를 대신하여 인시던트 기록 및 관련 리소스를 관리할 권한을 부여합니다.

AWSIncidentManagerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 10일, 03:34 UTC
- 편집된 시간: 2022년 12월 5일, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoT1ClickFullAccess

설명: AWS IoT 1-Click에 대한 전체 액세스를 제공합니다.

AWSIoT1ClickFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoT1ClickFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 11일, 22:10 UTC
- 편집된 시간: 2018년 5월 11일, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoT1ClickReadOnlyAccess

설명: AWS IoT 1-Click에 대한 읽기 전용 액세스를 제공합니다.

AWSIoT1ClickReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoT1ClickReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 11일, 21:49 UTC
- 편집된 시간: 2018년 5월 11일, 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
    }
  ],
}
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTAnalyticsFullAccess

설명: IoT Analytics에 대한 전체 액세스 권한을 제공합니다.

AWSIoTAnalyticsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTAnalyticsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 18일, 23:02 UTC
- 편집된 시간: 2018년 6월 18일, 23:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTAnalyticsReadOnlyAccess

설명: IoT Analytics에 대한 읽기 전용 액세스를 제공합니다.

AWSIoTAnalyticsReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTAnalyticsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 18일, 21:37 UTC
- 편집된 시간: 2018년 6월 18일, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTConfigAccess

설명: 이 정책은 AWS IoT 구성 작업에 대한 전체 액세스 권한을 제공합니다.

AWSIoTConfigAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTConfigAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:52 UTC
- 편집된 시간: 2019년 9월 27일, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTConfigReadOnlyAccess

설명: 이 정책은 AWS IoT 구성 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSIoTConfigReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTConfigReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:52 UTC
- 편집된 시간: 2019년 9월 27일, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDataAccess

설명: 이 정책은 AWS IoT 메시징 작업에 대한 전체 액세스 권한을 제공합니다.

AWSIoTDataAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDataAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:51 UTC
- 편집된 시간: 2021년 6월 23일, 21:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

설명: ADD_THINGS_TO_THING_GROUP 완화 조치를 실행을 위해 IoT 사물 그룹에 대한 쓰기 액세스 권한 및 IoT 인증서에 대한 읽기 액세스 권한을 제공합니다.

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:55 UTC
- 편집된 시간: 2019년 8월 7일, 17:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderAudit

설명: IoT 및 관련 리소스에 대한 읽기 액세스를 제공합니다.

AWSIoTDeviceDefenderAudit [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderAudit를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 7월 18일, 21:17 UTC
- 편집된 시간: 2019년 11월 25일, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

설명: ENABLE_IOT_LOGGING 완화 조치 실행을 위한 IoT 로깅을 활성화하기 위한 액세스를 제공합니다.

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
```

```

    "*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "iot.amazonaws.com"
      ]
    }
  }
}
]
}
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

설명: PUBLISH_FINDING_TO_SNS 완화 조치 실행을 위해 SNS 주제에 대한 메시지 게시 액세스 권한을 제공합니다.

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

설명: REPLACE_DEFAULT_POLICY_VERSION 완화 조치 실행을 위한 IoT 정책에 대한 쓰기 액세스 권한을 제공합니다.

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "Effect" : "Allow",
    "Action" : [
      "iot:CreatePolicyVersion"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

설명: UPDATE_CA_CERTIFICATE 완화 조치 실행을 위한 IoT CA 인증서에 대한 쓰기 액세스 권한을 제공합니다.

AWSIoTDeviceDefenderUpdateCACertMitigationAction [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderUpdateCACertMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:05 UTC
- 편집된 시간: 2019년 8월 7일, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

설명: UPDATE_DEVICE_CERTIFICATE 완화 조치 실행을 위한 IoT 인증서에 대한 쓰기 액세스 권한을 제공합니다.

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:06 UTC
- 편집된 시간: 2019년 8월 7일, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

설명: AWS IoT 디바이스 테스터가 IoT, S3 및 IAM을 포함한 서비스에 대한 액세스를 허용하여 FreeRTOS 검증 제품군을 실행할 수 있도록 합니다.

AWSIoTDeviceTesterForFreeRTOSFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceTesterForFreeRTOSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 12일, 20:33 UTC
- 편집된 시간: 2023년 8월 10일, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Statement" : [
  {
    "Sid" : "VisualEditor0",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/idt-*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "iot.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "VisualEditor1",
    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteThing",
      "iot:AttachThingPrincipal",
      "iot:DeleteCertificate",
      "iot:GetRegistrationCode",
      "iot:CreatePolicy",
      "iot:UpdateCACertificate",
      "s3:ListBucket",
      "iot:DescribeEndpoint",
      "iot:CreateOTAUpdate",
      "iot:CreateStream",
      "signer:ListSigningJobs",
      "acm:ListCertificates",
      "iot:CreateKeysAndCertificate",
      "iot:UpdateCertificate",
      "iot:CreateCertificateFromCsr",
      "iot:DetachThingPrincipal",
      "iot:RegisterCACertificate",
      "iot:CreateThing",
      "iam:ListRoles",
      "iot:RegisterCertificate",
      "iot:DeleteCACertificate",
      "signer:PutSigningProfile",
      "s3:ListAllMyBuckets",
      "signer:ListSigningPlatforms",
      "iot-device-tester:SendMetrics",
      "iot-device-tester:SupportedVersion",
      "iot-device-tester:LatestIdt",
      "iot-device-tester:CheckVersion",
```

```
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor2",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "signer:StartSigningJob",
    "acm:GetCertificate",
    "signer:DescribeSigningJob",
    "s3:CreateBucket",
    "execute-api:Invoke",
    "s3>DeleteBucket",
    "s3:PutBucketVersioning",
    "signer:CancelSigningProfile"
  ],
  "Resource" : [
    "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
    "arn:aws:signer:*:*:/signing-profiles/*",
    "arn:aws:signer:*:*:/signing-jobs/*",
    "arn:aws:iam:*:*:role/idt-*",
    "arn:aws:acm:*:*:certificate/*",
    "arn:aws:s3:::idt-*",
    "arn:aws:s3:::afr-ota*"
  ]
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",
  "Action" : [
    "iot>DeleteStream",
    "iot>DeleteCertificate",
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "iot>DeletePolicy",
    "s3:ListBucketVersions",
    "iot:UpdateCertificate",
    "iot:GetOTAUpdate",
    "iot>DeleteOTAUpdate",
    "iot:DescribeJobExecution"
  ],
  "Resource" : [
```

```

    "arn:aws:s3:::afr-ota*",
    "arn:aws:iot:*:*:thinggroup/idt*",
    "arn:aws:iam:*:*:role/idt-*"
  ]
},
{
  "Sid" : "VisualEditor4",
  "Effect" : "Allow",
  "Action" : [
    "iot:DeleteCertificate",
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "s3:DeleteObjectVersion",
    "iot:DeleteOTAUpdate",
    "s3:PutObject",
    "s3:GetObject",
    "iot:DeleteStream",
    "iot:DeletePolicy",
    "s3:DeleteObject",
    "iot:UpdateCertificate",
    "iot:GetOTAUpdate",
    "s3:GetObjectVersion",
    "iot:DescribeJobExecution"
  ],
  "Resource" : [
    "arn:aws:s3:::afr-ota*/**",
    "arn:aws:s3:::idt-*/**",
    "arn:aws:iot:*:*:policy/idt*",
    "arn:aws:iam:*:*:role/idt-*",
    "arn:aws:iot:*:*:otaupdate/idt*",
    "arn:aws:iot:*:*:thing/idt*",
    "arn:aws:iot:*:*:cert/**",
    "arn:aws:iot:*:*:job/**",
    "arn:aws:iot:*:*:stream/**"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : [

```

```
    "arn:aws:s3:::afr-ota*/**",
    "arn:aws:s3:::idt-*/**"
  ]
},
{
  "Sid" : "VisualEditor6",
  "Effect" : "Allow",
  "Action" : [
    "iot:CancelJobExecution"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/**",
    "arn:aws:iot:*:*:thing/idt*"
  ]
},
{
  "Sid" : "VisualEditor7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/**"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/**"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/Owner" : "IoTDeviceTester"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "VisualEditor9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/Owner" : "IoTDeviceTester"
      }
    }
  },
  {
    "Sid" : "VisualEditor10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:key-pair/*",
      "arn:aws:ec2:*:*:placement-group/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*"
    ]
  },
  {
    "Sid" : "VisualEditor11",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
```

```
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  },
  {
    "Sid" : "VisualEditor12",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "ssm:DescribeParameters",
      "ssm:GetParameters"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VisualEditor13",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "Owner"
        ]
      },
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances",
          "CreateSecurityGroup"
        ]
      }
    }
  }
]
```


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTDeviceTesterForGreengrassFullAccess

설명: AWS IoT 디바이스 테스터가 Lambda, IoT, API Gateway, IAM을 포함한 관련 서비스에 대한 액세스를 허용하여 AWS Greengrass 인증 제품군을 실행할 수 있도록 합니다.

AWSIoTDeviceTesterForGreengrassFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceTesterForGreengrassFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 20일, 21:21 UTC
- 편집된 시간: 2020년 6월 25일, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTEventsFullAccess

설명: IoT Events에 대한 전체 액세스 권한을 제공합니다.

AWSIoTEventsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTEventsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 10일, 22:51 UTC
- 편집된 시간: 2019년 1월 10일, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTEventsReadOnlyAccess

설명: IoT Events에 대한 읽기 전용 액세스를 제공합니다.

AWSIoTEventsReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTEventsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 10일, 22:50 UTC
- 편집된 시간: 2019년 9월 23일, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "iotevents:Describe*",
    "iotevents:List*"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoT FleetHub FederationAccess

설명: IoT 플릿 허브 애플리케이션을 위한 페더레이션 액세스

AWSIoT FleetHub FederationAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoT FleetHub FederationAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 15일, 08:08 UTC
- 편집된 시간: 2022년 4월 4일, 18:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoT FleetHub FederationAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoT FleetwiseServiceRolePolicy

설명: 보조 기능을 위해 사용하거나 관리하는 AWS AWSIoT Fleetwise 리소스 및 메타데이터에 권한을 부여합니다.

AWSIoT FleetwiseServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 21일, 23:27 UTC
- 편집된 시간: 2022년 9월 21일, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT FleetwiseServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/IoTFleetWise"
      ]
    }
  }
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTFullAccess

설명: 이 정책은 AWS IoT 구성 및 메시징 작업에 대한 전체 액세스 권한을 제공합니다.

AWSIoTFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 8일, 15:19 UTC
- 편집된 시간: 2022년 5월 19일, 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTLogging

설명: Amazon CloudWatch Log 그룹을 생성하고 로그를 그룹으로 스트리밍할 수 있습니다.

AWSIoTLogging [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTLogging를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 10월 8일, 15:17 UTC
- 편집된 시간: 2015년 10월 8일, 15:17 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTOTAUpdate

설명: AWS IoT Job을 생성하고 AWS 코드 서명자 작업을 설명할 수 있는 액세스 권한을 허용합니다.

AWSIoTOTAUpdate [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTOTAUpdate를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 12월 20일, 20:36 UTC
- 편집된 시간: 2017년 12월 20일, 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTRoboRunnerFullAccess

설명: 이 정책은 AWS IoT에 대한 전체 액세스를 허용하는 권한을 RoboRunner 부여합니다.

AWSIoTRoboRunnerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTRoboRunnerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 03:54 UTC
- 편집된 시간: 2023년 2월 23일, 18:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTRoboRunnerReadOnly

설명: 이 정책은 AWS RoboRunner IoT에 대한 읽기 전용 액세스를 허용하는 권한을 부여합니다.

AWSIoTRoboRunnerReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTRoboRunnerReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 03:43 UTC

- 편집된 시간: 2022년 11월 16일, 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTRoboRunnerServiceRolePolicy

설명: AWS RoboRunner IoT가 고객을 대신하여 관련 AWS 리소스를 관리할 수 있도록 합니다.

AWSIoTRoboRunnerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 2월 21일, 16:56 UTC
- 편집된 시간: 2023년 2월 21일, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Usage"
      ]
    }
  }
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTRuleActions

설명: AWS IoT 규칙 동작에서 지원되는 모든 AWS 서비스에 액세스할 수 있습니다.

AWSIoTRuleActions [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTRuleActions를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 10월 8일, 15:14 UTC
- 편집된 시간: 2018년 1월 16일, 19:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTSiteWiseConsoleFullAccess

설명: 를 SiteWise 사용하여 AWS IoT를 관리할 수 있는 전체 액세스 권한을 제공합니다 AWS Management Console. 이 정책은 또한 AWS IoT와 함께 사용되는 데이터 저장소 SiteWise (예: IoT Analytics) 를 생성 및 나열할 수 있는 액세스 권한, AWS AWS IoT Greengrass 리소스를 나열하고 볼 수 있는 액세스 권한, AWS Secrets Manager 암호를 나열 및 수정하고, AWS IoT 사물 그림자를 검색하고, 특정 태그가 포함된 리소스를 나열하고, IoT를 위한 서비스 연결 역할을 생성 및 사용할 수 있는 액세스 권한을 부여합니다. AWS SiteWise

AWSIoTSiteWiseConsoleFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTSiteWiseConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 31일, 21:37 UTC
- 편집된 시간: 2019년 5월 31일, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "iot:DescribeEndpoint",
    "iot:GetThingShadow"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:ListGroups"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "secretsmanager:ListSecrets",
    "secretsmanager:CreateSecret"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "secretsmanager:UpdateSecret"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
},
{
  "Action" : [
    "tag:GetResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Effect" : "Allow",
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "iotsitewise.amazonaws.com"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTSiteWiseFullAccess

설명: IoT에 대한 전체 액세스를 제공합니다 SiteWise.

AWSIoTSiteWiseFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTSiteWiseFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 4일, 20:53 UTC
- 편집된 시간: 2018년 12월 4일, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTSiteWiseMonitorPortalAccess

설명: 이 정책은 AWS IoT SiteWise 자산 및 자산 데이터에 액세스하고, IoT SiteWise Monitor 리소스를 만들고 AWS, AWS SSO 사용자를 나열할 수 있는 권한을 부여합니다.

AWSIoTSiteWiseMonitorPortalAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTSiteWiseMonitorPortalAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 5월 19일, 20:01 UTC
- 편집된 시간: 2020년 5월 19일, 20:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

설명: 이 역할은 AWS IoT SiteWise 모니터에게 IoT SiteWise 자산 및 자산 자산에 액세스하고 AWS IoT 포털을 통해 AWS IoT SiteWise 프로젝트, 대시보드 및 액세스 정책을 생성할 수 있는 권한을 부여합니다. AWS SiteWise

AWSIoTSiteWiseMonitorServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 14일, 00:59 UTC
- 편집된 시간: 2019년 12월 13일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTSiteWiseReadOnlyAccess

설명: IoT에 대한 읽기 전용 액세스를 제공합니다 SiteWise.

AWSIoTSiteWiseReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTSiteWiseReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 12월 4일, 20:55 UTC
- 편집된 시간: 2022년 9월 16일, 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTThingsRegistration

설명: 이 정책을 통해 사용자는 AWS IoT StartThingRegistrationTask API를 사용하여 대량으로 항목을 등록할 수 있습니다.

AWSIoTThingsRegistration [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTThingsRegistration를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 12월 1일, 20:21 UTC
- 편집된 시간: 2020년 10월 5일, 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTtwinMakerServiceRolePolicy

설명: AWS TwinMaker IoT가 사용자를 대신하여 다른 AWS 서비스를 호출하고 해당 리소스를 동기화할 수 있도록 합니다.

AWSIoTtwinMakerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 13일, 18:59 UTC
- 편집된 시간: 2023년 11월 13일, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessDataAccess

설명: AWS IoT Wireless 장치에 대한 관련 ID 데이터 액세스를 허용합니다.

AWSIoTWirelessDataAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessDataAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:31 UTC
- 편집된 시간: 2020년 12월 15일, 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessFullAccess

설명: 연결된 ID가 모든 AWS IoT Wireless 작업에 완전히 액세스할 수 있도록 합니다.

AWSIoTWirelessFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:27 UTC
- 편집된 시간: 2020년 12월 15일, 15:27 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessFullPublishAccess

설명: 사용자를 대신하여 IoT 규칙 엔진에 게시할 수 있는 IoT Wireless 전체 액세스 권한을 제공합니다.

AWSIoTWirelessFullPublishAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessFullPublishAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:29 UTC
- 편집된 시간: 2020년 12월 15일, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessGatewayCertManager

설명: 연결된 ID 액세스를 통해 IoT 인증서를 생성, 나열 및 설명할 수 있습니다.

AWSIoTWirelessGatewayCertManager [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessGatewayCertManager를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:30 UTC
- 편집된 시간: 2020년 12월 15일, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "iot:CreateKeysAndCertificate",
    "iot:DescribeCertificate",
    "iot:ListCertificates"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessLogging

설명: 연결된 ID로 Amazon CloudWatch Logs 그룹을 생성하고 로그를 그룹으로 스트리밍할 수 있도록 허용합니다.

AWSIoTWirelessLogging [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessLogging를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:32 UTC
- 편집된 시간: 2020년 12월 15일, 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIoTWirelessReadOnlyAccess

설명: AWS IoT 무선에 대한 관련 ID 읽기 전용 액세스를 허용합니다.

AWSIoTWirelessReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:28 UTC
- 편집된 시간: 2020년 12월 15일, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIPAMServiceRolePolicy

설명: VPC IP 주소 관리자가 사용자를 대신하여 VPC 리소스에 액세스하고 AWS 조직과 통합할 수 있습니다.

AWSIPAMServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 30일, 19:08 UTC
- 편집된 시간: 2023년 11월 8일, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIQContractServiceRolePolicy

설명: AWS IQ에서 고객을 대신하여 결제 요청을 실행하는 데 사용됩니다.

AWSIQContractServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 22일, 19:28 UTC
- 편집된 시간: 2019년 8월 22일, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIQFullAccess

설명: AWS IQ에 대한 전체 액세스 권한 제공

AWSIQFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSIQFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 4일, 23:13 UTC
- 편집된 시간: 2019년 9월 25일, 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSIQPermissionServiceRolePolicy

설명: AWS IQ 전문가가 맡는 역할을 IQ가 관리할 수 있도록 합니다. AWS

AWSIQPermissionServiceRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 22일, 19:36 UTC
- 편집된 시간: 2019년 8월 22일, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

설명: AWS KMS 사용자 지정 키 스토어에 필요한 AWS 서비스 및 리소스에 액세스할 수 있습니다.

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 20:10 UTC
- 편집된 시간: 2023년 11월 10일, 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

설명: AWS KMS가 다중 지역 키의 공유 속성을 동기화할 수 있도록 합니다.

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 16일, 15:37 UTC
- 편집된 시간: 2021년 6월 16일, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSKeyManagementServicePowerUser

설명: KMS (AWS 키 관리 서비스)에 대한 액세스를 제공합니다.

AWSKeyManagementServicePowerUser [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSKeyManagementServicePowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2017년 3월 7일, 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLakeFormationCrossAccountManager

설명: Lake Formation을 통해 Glue 리소스에 대한 크로스 계정 액세스를 제공합니다. 또한 조직 및 리소스 액세스 관리자와 같은 기타 필수 서비스에 대한 읽기 액세스를 부여합니다.

AWSLakeFormationCrossAccountManager [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLakeFormationCrossAccountManager를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 4일, 20:59 UTC
- 편집 시간: 2024년 3월 22일 18:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram>DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```

        "ram:ResourceShareName" : [
            "LakeFormation*"
        ]
    }
}
},
{
    "Sid" : "AllowManageResourceSharePermissions",
    "Effect" : "Allow",
    "Action" : [
        "ram:AssociateResourceSharePermission"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ram:PermissionArn" : [
                "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
            ]
        }
    }
},
{
    "Sid" : "AllowXAcctManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "glue:PutResourcePolicy",
        "glue>DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowOrganizationsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
    ],
    "Resource" : "*"
}
}

```

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLakeFormationDataAdmin

설명: 데이터 레이크를 관리하기 위해 AWS Lake Formation 및 AWS Glue와 같은 관련 서비스에 대한 관리자 액세스 권한을 부여합니다.

AWSLakeFormationDataAdmin [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLakeFormationDataAdmin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 8월 8일, 17:33 UTC
- 편집 시간: 2024년 3월 22일 18:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambda_FullAccess

설명: Lambda 서비스, AWS AWS Lambda 콘솔 기능 및 기타 관련 서비스에 대한 전체 액세스 권한을 부여합니다. AWS

AWSLambda_FullAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSLambda_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 17일, 21:14 UTC
- 편집된 시간: 2020년 11월 17일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambda_ReadOnlyAccess

설명: Lambda 서비스 AWS , AWS Lambda 콘솔 기능 및 기타 관련 서비스에 대한 읽기 전용 액세스 권한을 부여합니다. AWS

AWSLambda_ReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambda_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 17일, 21:10 UTC
- 편집된 시간: 2023년 7월 27일, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaBasicExecutionRole

설명: CloudWatch 로그에 쓰기 권한을 제공합니다.

AWSLambdaBasicExecutionRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaBasicExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:03 UTC
- 편집된 시간: 2015년 4월 9일, 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaDynamoDBExecutionRole

설명: DynamoDB 스트림에 대한 목록 및 읽기 액세스와 로그에 대한 쓰기 권한을 제공합니다.
CloudWatch

AWSLambdaDynamoDBExecutionRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaDynamoDBExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:09 UTC
- 편집된 시간: 2015년 4월 9일, 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "Action" : [
      "dynamodb:DescribeStream",
      "dynamodb:GetRecords",
      "dynamodb:GetShardIterator",
      "dynamodb:ListStreams",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaENIManagementAccess

설명: VPC 지원 Lambda 함수에서 사용하는 ENI를 관리 (생성, 설명, 삭제) 하기 위한 Lambda 함수에 대한 최소 권한을 제공합니다.

AWSLambdaENIManagementAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaENIManagementAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 6일, 00:37 UTC
- 편집된 시간: 2020년 10월 1일, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaExecute

설명: Put, Get, S3에 대한 액세스 권한 및 CloudWatch 로그에 대한 전체 액세스 권한을 제공합니다.

AWSLambdaExecute [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaExecute를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3::*:*"
    }
  ]
}
```

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaFullAccess

설명: 이 정책은 지원 중단될 예정입니다. 지침은 설명서 <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>을 참조하십시오. Lambda, S3, DynamoDB, 지표 및 로그에 대한 전체 액세스를 제공합니다. CloudWatch

AWSLambdaFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2017년 11월 27일, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaInvocation-DynamoDB

설명: DynamoDB 스트림에 대한 읽기 액세스를 제공합니다.

AWSLambdaInvocation-DynamoDB [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaInvocation-DynamoDB를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaKinesisExecutionRole

설명: Kinesis 스트림에 대한 목록 및 읽기 액세스 권한과 로그에 CloudWatch 대한 쓰기 권한을 제공합니다.

AWSLambdaKinesisExecutionRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaKinesisExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:14 UTC
- 편집된 시간: 2018년 11월 19일, 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaMSKExecutionRole

설명: VPC 내의 MSK 클러스터에 액세스하고, VPC에서 ENI를 관리 (생성, 설명, 삭제) 하고, 로그에 권한을 쓰는 데 필요한 권한을 제공합니다. CloudWatch

AWSLambdaMSKExecutionRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaMSKExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 11일, 17:35 UTC
- 편집된 시간: 2022년 8월 2일, 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaReplicator

설명: Lambda Replicator에 함수를 리전 간에 복제하는 데 필요한 권한을 부여합니다.

AWSLambdaReplicator [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 5월 23일, 17:53 UTC
- 편집된 시간: 2017년 12월 8일, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaRole

설명: AWS Lambda 서비스 역할에 대한 기본 정책입니다.

AWSLambdaRole [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaSQSQueueExecutionRole

설명: SQS 대기열에 대한 수신, 메시지 삭제, 속성 읽기 액세스, 로그에 대한 쓰기 권한을 제공합니다.
CloudWatch

AWSLambdaSQSQueueExecutionRole [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaSQSQueueExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 6월 14일, 21:50 UTC
- 편집된 시간: 2018년 6월 14일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLambdaVPCAccessExecutionRole

설명: VPC 내에서 리소스에 액세스하는 동안 Lambda 함수를 실행할 수 있는 최소 권한 (네트워크 인터페이스를 생성, 설명, 삭제하고 로그에 대한 쓰기 권한) 을 제공합니다. CloudWatch

AWSLambdaVPCAccessExecutionRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaVPCAccessExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 11일, 23:15 UTC
- 편집 시간: 2024년 1월 5일 22:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerConsumptionPolicy

설명: 사용자에게 사용 권한이 있는 AWS 라이선스에서 사용하는 데 필요한 License Manager API 작업에 액세스할 수 있는 권한을 제공합니다.

AWSLicenseManagerConsumptionPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLicenseManagerConsumptionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 8월 11일, 23:18 UTC
- 편집된 시간: 2021년 8월 11일, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

설명: AWS License Manager Linux 구독 서비스가 사용자를 대신하여 리소스를 관리할 수 있도록 합니다.

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2022년 12월 20일, 18:54 UTC
- 편집된 시간: 2022년 12월 20일, 18:54 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerMasterAccountRolePolicy

설명: AWS License Manager 서비스 마스터 계정 역할 정책

AWSLicenseManagerMasterAccountRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:03 UTC
- 편집된 시간: 2022년 5월 31일, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerMemberAccountRolePolicy

설명: AWS License Manager 서비스 멤버 계정 역할 정책

AWSLicenseManagerMemberAccountRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:04 UTC
- 편집된 시간: 2019년 11월 15일, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerServiceRolePolicy

설명: AWS License Manager 서비스 기본 역할 정책

AWSLicenseManagerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:02 UTC
- 편집된 시간: 2021년 7월 30일, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

설명: AWS License Manager 사용자 구독 서비스가 사용자를 대신하여 리소스를 관리할 수 있도록 합니다.

AWSLicenseManagerUserSubscriptionsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 30일, 01:17 UTC
- 편집된 시간: 2022년 11월 21일, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSM2ServicePolicy

설명: AWS M2가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

AWSM2ServicePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 7일, 20:26 UTC
- 편집된 시간: 2022년 6월 7일, 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSManagedServices_ContactsServiceRolePolicy

설명: AWS Managed Services가 AWS 리소스의 태그 값을 읽을 수 있도록 허용합니다.

AWSManagedServices_ContactsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 23일, 17:07 UTC
- 편집된 시간: 2023년 3월 23일, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  },
  "NumericGreaterThanOrEqualTo" : {
    "s3:TlsVersion" : "1.2"
  }
}
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

설명: AWS Managed Services - 탐정 제어 인프라를 관리하는 정책

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 12월 19일, 23:11 UTC
- 편집된 시간: 2022년 12월 19일, 23:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSManagedServices_EventsServiceRolePolicy

설명: AMS 이벤트 프로세서 기능을 활성화하기 위한 AWS Managed Services 정책입니다.

AWSManagedServices_EventsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 2월 7일, 18:41 UTC
- 편집된 시간: 2023년 2월 7일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSManagedServicesDeploymentToolkitPolicy

설명: AWS Managed Services에서 사용자 대신 배포 툴킷을 관리할 수 있도록 허용합니다.

AWSManagedServicesDeploymentToolkitPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 9일, 18:33 UTC
- 편집 시간: 2024년 4월 4일 20:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceAmiIngestion

설명: Amazon 머신 이미지 (AMI) 를 AWS Marketplace 복사하여 목록에 올릴 수 있습니다. AWS Marketplace

AWSMarketplaceAmiIngestion [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceAmiIngestion를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 25일, 20:55 UTC
- 편집된 시간: 2020년 9월 25일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceDeploymentServiceRolePolicy

설명: AWS Marketplace 구독하는 제품에 대한 셀러 배포 매개변수를 생성하고 관리할 수 AWS Marketplace 있습니다.

AWSMarketplaceDeploymentServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 15일, 23:34 UTC
- 편집된 시간: 2023년 11월 15일, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
    }
  }
}
]

```

```
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceFullAccess

설명: AWS Marketplace 소프트웨어 구독 및 구독 취소 기능을 제공하고, 사용자가 Marketplace 'Your Software' 페이지에서 Marketplace 소프트웨어 인스턴스를 관리할 수 있도록 하며, EC2에 대한 관리 액세스를 제공합니다.

AWSMarketplaceFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 11일, 17:21 UTC
- 편집된 시간: 2022년 3월 4일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceGetEntitlements

설명: 권한에 대한 읽기 액세스 AWS Marketplace 권한을 제공합니다.

AWSMarketplaceGetEntitlements [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceGetEntitlements를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 3월 27일, 19:37 UTC
- 편집 시간: 2024년 4월 5일 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AWSMarketplaceGetEntitlements",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:GetEntitlements"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceImageBuildFullAccess

설명: AWS Marketplace 프라이빗 이미지 빌드 기능에 대한 전체 액세스 권한을 제공합니다. 프라이빗 이미지를 생성하는 것 외에도 이미지에 태그를 추가하고, ec2 인스턴스를 시작 및 종료할 수 있는 권한도 제공합니다.

AWSMarketplaceImageBuildFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceImageBuildFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 7월 31일, 23:29 UTC
- 편집된 시간: 2022년 3월 4일, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

설명: 라이선스 관리를 위해 AWS 서비스 사용하거나 관리하는 AWS Marketplace 리소스에 액세스할 수 있도록 합니다.

AWSMarketplaceLicenseManagementServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 3일, 08:33 UTC
- 편집된 시간: 2020년 12월 3일, 08:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceManageSubscriptions

설명: 소프트웨어 구독 및 구독 취소 기능을 제공합니다. AWS Marketplace

AWSMarketplaceManageSubscriptions [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceManageSubscriptions를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 1월 19일, 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceMeteringFullAccess

설명: AWS Marketplace 미터링에 대한 전체 액세스 권한을 제공합니다.

AWSMarketplaceMeteringFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceMeteringFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 3월 17일, 22:39 UTC
- 편집된 시간: 2016년 3월 17일, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceMeteringRegisterUsage

설명: AWS Marketplace Metering Service를 통해 리소스를 등록하고 사용량을 추적할 수 있는 권한을 제공합니다.

AWSMarketplaceMeteringRegisterUsage [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceMeteringRegisterUsage를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 21일, 01:17 UTC
- 편집된 시간: 2019년 11월 21일, 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceProcurementSystemAdminFullAccess

설명: AWS Marketplace eProcurement 통합을 위한 모든 관리 작업에 대한 전체 액세스 권한을 제공합니다.

AWSMarketplaceProcurementSystemAdminFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceProcurementSystemAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 25일, 13:07 UTC
- 편집된 시간: 2019년 6월 25일, 13:07 UTC
- ARN: arn:aws:iam::aws:policy/
AWSMarketplaceProcurementSystemAdminFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

설명: AWS Marketplace 서비스에 액세스하여 구매 주문 관리를 수행할 수 있습니다.

AWSMarketplacePurchaseOrdersServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 27일, 15:12 UTC
- 편집된 시간: 2021년 10월 27일, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceRead-only

설명: AWS Marketplace 구독을 검토할 수 있는 기능을 제공합니다.

AWSMarketplaceRead-only [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceRead-only를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 1월 19일, 23:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

설명: 재판매 승인을 위해 사용하거나 관리하는 리소스에 AWS Marketplace 대한 액세스 AWS 서비스 및 리소스를 활성화합니다.

AWSMarketplaceResaleAuthorizationServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 3월 5일 18:47 UTC
- 편집 시간: 2024년 3월 5일 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceSellerFullAccess

설명: AMI 관리와 같은 기타 AWS 서비스의 모든 셀러 작업에 대한 전체 액세스 권한을 제공합니다.
AWS Marketplace

AWSMarketplaceSellerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceSellerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 2일, 20:40 UTC
- 편집 시간: 2024년 3월 15일 16:09 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceSellerProductsFullAccess

설명: 셀러에게 AWS Marketplace 관리 제품 페이지 및 AMI 관리와 같은 기타 AWS 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSMarketplaceSellerProductsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceSellerProductsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 2일, 21:06 UTC
- 편집된 시간: 2023년 7월 18일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMarketplaceSellerProductsReadOnly

설명: 셀러에게 AWS Marketplace 관리 제품 페이지에 대한 읽기 전용 액세스 권한을 제공합니다.

AWSMarketplaceSellerProductsReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceSellerProductsReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 2일, 21:40 UTC
- 편집된 시간: 2022년 11월 19일, 00:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMediaConnectServicePolicy

설명: 사용하거나 관리하는 리소스에 대한 액세스 AWS 서비스 및 리소스를 활성화하는 기본 MediaConnect 정책입니다.

AWSMediaConnectServicePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 3일, 22:11 UTC
- 편집된 시간: 2023년 4월 3일, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMediaTailorServiceRolePolicy

설명: 에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다. MediaTailor

AWSMediaTailorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 17일, 22:27 UTC
- 편집된 시간: 2021년 9월 17일, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubDiscoveryAccess

설명: 정책을 통해 고객을 AWSMigrationHubService AWSApplicationDiscoveryService 대신하여 전화를 걸 수 있습니다.

AWSMigrationHubDiscoveryAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubDiscoveryAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:30 UTC
- 편집된 시간: 2020년 8월 6일, 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubDMSAccess

설명: Database Migration Service가 고객 계정에서 역할을 맡아 Migration Hub에 전화를 걸도록 하는 정책

AWSMigrationHubDMSAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubDMSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 14:00 UTC
- 편집된 시간: 2019년 10월 7일, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubFullAccess

설명: 고객에게 Migration Hub 서비스에 대한 액세스를 제공하는 관리형 정책

AWSMigrationHubFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 14:02 UTC
- 편집된 시간: 2019년 6월 19일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


- 생성 시간: 2022년 4월 20일, 02:26 UTC
- 편집 시간: 2023년 12월 5일 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

설명: 당사 서비스가 S3에서 스크립트를 다운로드하여 인스턴스를 오케스트레이션하고 EC2 인스턴스 내에서 비밀 값을 가져오려면 이 정책을 SAP와 MGN으로 마이그레이션한 인스턴스에 연결해야 합니다.

AWSMigrationHubOrchestratorInstanceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubOrchestratorInstanceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 20일, 02:43 UTC
- 편집된 시간: 2022년 4월 20일, 02:43 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubOrchestratorPlugin

설명: AWS Migration Hub Orchestrator를 위한 Amazon 심플 스토리지 서비스, AWS Secrets Manager 및 플러그인 관련 작업에 대한 제한된 액세스를 제공합니다.

AWSMigrationHubOrchestratorPlugin [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubOrchestratorPlugin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 20일, 02:25 UTC
- 편집된 시간: 2022년 4월 20일, 02:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
```

```
    "s3:GetObject",
    "s3:GetBucketAcl"
  ],
  "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "execute-api:Invoke",
    "execute-api:ManageConnections"
  ],
  "Resource" : [
    "arn:aws:execute-api:*:*:*/*prod/*/put-log-data",
    "arn:aws:execute-api:*:*:*/*prod/*/put-metric-data"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "migrationhub-orchestrator:RegisterPlugin",
    "migrationhub-orchestrator:GetMessage",
    "migrationhub-orchestrator:SendMessage"
  ],
  "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
}
]
```


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubOrchestratorServiceRolePolicy

설명: Migration Hub Orchestrator가 온프레미스 워크로드를 마이그레이션하고 현대화하는 데 필요한 권한을 제공합니다.

AWSMigrationHubOrchestratorServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 4월 20일, 02:24 UTC
- 편집 시간: 2024년 3월 4일 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

설명: 네트워크 브리지가 없는 환경을 사용할 때는 필요하지 않은 AWS Transit Gateway 및 EC2 보안 그룹을 제외한 AWS Migration Hub Refactor Spaces 및 기타 AWS 관련 서비스에 대한 전체 액세스 권한을 부여합니다. 또한 이 정책은 AWS Lambda 및 Resource Access AWS Manager에 필요한 권한을 제외합니다. 태그를 기반으로 범위를 좁힐 수 있기 때문입니다.

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 3일, 20:09 UTC
- 편집 시간: 2024년 4월 11일 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

설명: SSM 자동화 문서에 AWSRefactorSpaces 전달된 IAM 서비스 역할에서 자동화 실행에 필요한 권한을 부여하는 CreateResources 데 사용합니다. 이 정책은 자동화 진행 상황을 추적하기 위해 EC2 태그에 대한 읽기/쓰기 액세스를 부여합니다. 또한 Refactor Spaces 환경의 네트워크 브리지가 활성화되면 자동화는 환경의 보안 그룹을 EC2 인스턴스에 추가하여 환경의 다른 Refactor Spaces 서비스로부터의 트래픽을 허용합니다. 또한 이 정책은 Application Migration Service의 시작 후 작업 SSM 파라미터에 대한 액세스를 부여합니다.

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubRefactorSpaces-SSMAutomationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 10일, 15:08 UTC
- 편집된 시간: 2023년 8월 10일, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubRefactorSpacesFullAccess

설명: 태그를 기반으로 범위를 좁힐 수 있으므로 AWS Lambda 및 Resource Access AWS Manager에 필요한 권한을 제외하고 AWS MigrationHub 리팩터링 스페이스, 리팩터링 스페이스 콘솔 기능 및 기타 관련 AWS 서비스에 대한 전체 액세스 권한을 부여합니다. AWS MigrationHub

AWSMigrationHubRefactorSpacesFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubRefactorSpacesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 07:12 UTC
- 편집 시간: 2024년 4월 11일 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

설명: AWS Migration Hub 리팩터링 AWS 스페이스에서 관리하거나 사용하는 리소스에 대한 액세스를 제공합니다.

AWSMigrationHubRefactorSpacesServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 29일, 06:50 UTC
- 편집된 시간: 2023년 7월 20일, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-
n1b-*"
  },
  {
    "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"
      }
    }
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubSMSAccess

설명: 서버 마이그레이션 서비스가 고객 계정에서 Migration Hub를 호출하는 역할을 담당하도록 하는 정책

AWSMigrationHubSMSAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubSMSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:57 UTC
- 편집된 시간: 2019년 10월 7일, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubStrategyCollector

설명: AWS Migration Hub 전략 권장 사항 서비스와의 통신, 서비스와 관련된 S3 버킷에 대한 읽기/쓰기 액세스, 로그와 지표를 업로드하기 위한 Amazon API Gateway 액세스, 자격 증명을 가져오기 위한 AWS Secrets Manager 액세스 및 기타 관련 서비스를 허용하는 권한을 부여합니다.

AWSMigrationHubStrategyCollector [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubStrategyCollector를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 19일, 20:15 UTC
- 편집 시간: 2024년 4월 1일 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubStrategyConsoleFullAccess

설명: AWS Migration Hub 전략 권장 사항 서비스에 대한 전체 액세스 권한과 를 통해 관련 AWS 서비스에 대한 액세스 권한을 AWS Management Console부여합니다.

AWSMigrationHubStrategyConsoleFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubStrategyConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 19일, 20:13 UTC
- 편집된 시간: 2022년 11월 9일, 00:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMigrationHubStrategyServiceRolePolicy

설명: AWS Migration Hub 전략 권장 사항 서비스에서 사용하거나 관리하는 AWS 리소스에 액세스할 수 있도록 합니다.

AWSMigrationHubStrategyServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 19일, 20:02 UTC
- 편집된 시간: 2021년 10월 19일, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMobileHub_FullAccess

설명: AWS Mobile Hub에서 프로젝트 (및 관련 AWS 리소스) 를 생성, 삭제 및 수정할 수 있는 권한을 사용자에게 부여하기 위해 이 정책을 모든 사용자, 역할 또는 그룹에 첨부할 수 있습니다. 여기에는 각 Mobile Hub 프로젝트에 대한 샘플 모바일 앱 소스 코드를 생성하고 다운로드할 수 있는 권한도 포함됩니다.

AWSMobileHub_FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMobileHub_FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 5일, 19:56 UTC
- 편집된 시간: 2019년 12월 19일, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMobileHub_ReadOnly

설명: AWS Mobile Hub에서 프로젝트를 나열하고 볼 수 있는 권한을 사용자에게 부여하기 위해 이 정책을 모든 사용자, 역할 또는 그룹에 첨부할 수 있습니다. 여기에는 각 Mobile Hub 프로젝트에 대한 샘플 모바일 앱 소스 코드를 생성하고 다운로드할 수 있는 권한도 포함됩니다. 사용자는 Mobile Hub 프로젝트에 대한 구성을 수정할 수 없습니다.

AWSMobileHub_ReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMobileHub_ReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 5일, 19:55 UTC
- 편집된 시간: 2018년 7월 23일, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSMSKReplicatorExecutionRole

설명: Amazon MSK 리플리케이터에 MSK 클러스터 간에 데이터를 복제할 수 있는 권한을 부여합니다.

AWSMSKReplicatorExecutionRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSMSKReplicatorExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 작성 시간: 2023년 12월 6일 00:07 UTC
- 편집 시간: 2024년 3월 25일 21:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSNetworkFirewallServiceRolePolicy

설명: AWSNetworkFirewall 방화벽에 필요한 리소스를 만들고 관리할 수 있습니다.

AWSNetworkFirewallServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 17일, 17:17 UTC
- 편집된 시간: 2023년 3월 30일, 17:19 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*:*:vpce/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
      }
    }
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSNetworkManagerCloudWANServiceRolePolicy

설명: 코어 네트워크와 관련된 NetworkManager 리소스에 액세스할 수 있습니다.

AWSNetworkManagerCloudWANServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 12일, 12:17 UTC
- 편집된 시간: 2022년 7월 12일, 12:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
```

```
    "ec2:DisableTransitGatewayRouteTablePropagation"
  ],
  "Resource" : "*"
}
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSNetworkManagerFullAccess

설명: NetworkManager 를 통해 Amazon에 대한 전체 액세스 권한을 제공합니다 AWS Management Console.

AWSNetworkManagerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSNetworkManagerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 17:37 UTC
- 편집된 시간: 2019년 12월 3일, 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSNetworkManagerReadOnlyAccess

설명: NetworkManager 를 통해 Amazon에 대한 읽기 전용 액세스를 제공합니다 AWS Management Console.

AWSNetworkManagerReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 `AWSNetworkManagerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 17:35 UTC
- 편집된 시간: 2019년 12월 3일, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSNetworkManagerServiceRolePolicy

설명: 글로벌 네트워크와 관련된 NetworkManager 리소스에 액세스할 수 있습니다.

AWSNetworkManagerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 3일, 14:03 UTC
- 편집된 시간: 2022년 7월 27일, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorks_FullAccess

설명: 에 대한 전체 액세스 권한을 제공합니다 AWS OpsWorks.

AWSOpsWorks_FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorks_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 16:29 UTC
- 편집된 시간: 2021년 1월 22일, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksCloudWatchLogs

설명: CWLogs 통합이 활성화된 OpsWorks 인스턴스가 로그를 전송하고 필수 로그 그룹을 생성할 수 있도록 합니다.

AWSOpsWorksCloudWatchLogs [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksCloudWatchLogs를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 3월 30일, 17:47 UTC
- 편집된 시간: 2017년 3월 30일, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksCMInstanceProfileRole

설명: OpsWorks CM에서 시작한 인스턴스에 대한 S3 액세스를 제공합니다.

AWSOpsWorksCMInstanceProfileRole [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksCMInstanceProfileRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 24일, 09:48 UTC
- 편집된 시간: 2021년 4월 23일, 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksCMServiceRole

설명: OpsWorks CM 서버 생성에 사용할 서비스 역할 정책입니다.

AWSOpsWorksCMServiceRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksCMServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 24일, 09:49 UTC
- 편집된 시간: 2021년 4월 23일, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksInstanceRegistration

설명: Amazon EC2 인스턴스를 스택에 등록할 수 있는 액세스 권한을 제공합니다. AWS OpsWorks
AWSOpsWorksInstanceRegistration [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksInstanceRegistration를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 6월 3일, 14:23 UTC
- 편집된 시간: 2016년 6월 3일, 14:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    ]
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksRegisterCLI_EC2

설명: CLI를 통해 EC2 인스턴스를 등록할 수 있도록 하는 OpsWorks 정책

AWSOpsWorksRegisterCLI_EC2 [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksRegisterCLI_EC2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 18일, 15:56 UTC
- 편집된 시간: 2019년 6월 18일, 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOpsWorksRegisterCLI_OnPremises

설명: CLI를 통한 온프레미스 인스턴스 등록을 지원하는 정책 OpsWorks

AWSOpsWorksRegisterCLI_OnPremises [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksRegisterCLI_OnPremises를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 18일, 15:33 UTC
- 편집된 시간: 2019년 6월 18일, 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOrganizationsFullAccess

설명: Organizations에 AWS 대한 전체 액세스 권한을 제공합니다.

AWSOrganizationsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSOrganizationsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 6일, 20:31 UTC
- 편집 시간: 2024년 2월 6일 17:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOrganizationsReadOnlyAccess

설명: Organizations에 AWS 대한 읽기 전용 액세스를 제공합니다.

AWSOrganizationsReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSOrganizationsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 6일, 20:32 UTC
- 편집 시간: 2024년 6월 7일 21:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOrganizationsServiceTrustPolicy

설명: Organizations가 고객 구성을 단순화할 AWS 서비스 목적으로 승인된 다른 AWS 조직과 신뢰를 공유할 수 있도록 허용하는 정책입니다.

AWSOrganizationsServiceTrustPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 10일, 23:04 UTC
- 편집된 시간: 2017년 11월 1일, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOutpostsAuthorizeServerPolicy

설명: 이 정책은 온프레미스 네트워크에 Outpost 서버를 설치할 수 있는 권한을 부여합니다.

AWSOutpostsAuthorizeServerPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOutpostsAuthorizeServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 4일, 19:23 UTC
- 편집된 시간: 2023년 1월 4일, 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSOutpostsServiceRolePolicy

설명: AWS Outposts에서 관리하는 AWS 리소스에 액세스할 수 있도록 하는 서비스 연결 역할 정책

AWSOutpostsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 9일, 22:55 UTC

- 편집된 시간: 2020년 11월 9일, 22:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaApplianceRolePolicy

설명: AWS Panorama 어플라이언스의 AWS IoT 소프트웨어가 Amazon에 로그를 업로드할 수 있도록 허용합니다. CloudWatch

AWSPanoramaApplianceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaApplianceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:13 UTC
- 편집된 시간: 2020년 12월 1일, 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaApplianceServiceRolePolicy

설명: AWS Panorama 어플라이언스가 Amazon에 로그를 업로드하고 Panorama와 함께 사용하기 위해 생성된 Amazon S3 액세스 포인트에서 객체를 가져올 수 있도록 허용합니다. CloudWatch AWS

AWSPanoramaApplianceServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaApplianceServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 10월 20일, 12:14 UTC
- 편집된 시간: 2023년 1월 17일, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaFullAccess

설명: AWS Panorama에 대한 전체 액세스 권한을 제공합니다.

AWSPanoramaFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 13:12 UTC
- 편집된 시간: 2022년 1월 12일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaGreengrassGroupRolePolicy

설명: AWS Panorama 어플라이언스의 Lambda 함수가 Panorama의 리소스를 관리하고, 로그와 지표를 CloudWatch Amazon에 업로드하고, Panorama와 함께 사용하기 위해 생성된 버킷의 객체를 관리할 수 있도록 허용합니다. AWS

AWSPanoramaGreengrassGroupRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaGreengrassGroupRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:10 UTC
- 편집된 시간: 2021년 1월 6일, 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaSageMakerRolePolicy

설명: Amazon이 SageMaker AWS Panorama와 함께 사용하기 위해 생성된 버킷의 객체를 관리할 수 있도록 허용합니다.

AWSPanoramaSageMakerRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaSageMakerRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:13 UTC
- 편집된 시간: 2020년 12월 1일, 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3::*aws-panorama*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaServiceLinkedRolePolicy

설명: AWS 파노라마가 AWS IoT, AWS Secrets Manager 및 AWS 파노라마의 리소스를 관리할 수 있도록 합니다.

AWSPanoramaServiceLinkedRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 20일, 12:12 UTC
- 편집된 시간: 2021년 10월 20일, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPanoramaServiceRolePolicy

설명: AWS Panorama가 Amazon S3, IoT, AWS IoT, GreenGrass Lambda, Amazon 및 AWS Amazon CloudWatch Logs의 리소스를 관리하고 IoT, AWS IoT SageMaker 및 Amazon에 서비스 역할을 전달할 수 있도록 합니다. AWS GreenGrass SageMaker

AWSPanoramaServiceRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:14 UTC
- 편집된 시간: 2020년 12월 1일, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPriceListServiceFullAccess

설명: AWS 가격표 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSPriceListServiceFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPriceListServiceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 22일, 00:36 UTC
- 편집된 시간: 2017년 11월 22일, 00:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPriateCAAuditor

설명: 감사자에게 AWS 사설 인증 기관에 대한 액세스 권한을 제공합니다.

AWSPriateCAAuditor [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPriateCAAuditor를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:33 UTC
- 편집된 시간: 2023년 2월 14일, 18:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAAuditor

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPriateCAFullAccess

설명: AWS 사설 인증 기관에 대한 전체 액세스 권한을 제공합니다.

AWSPriateCAFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPriateCAFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:20 UTC
- 편집된 시간: 2023년 2월 14일, 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPrivateCAPrivilegedUser

설명: 권한 있는 인증서 사용자에게 AWS 사설 인증 기관에 대한 액세스 권한을 제공합니다.

AWSPrivateCAPrivilegedUser [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPrivateCAPrivilegedUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:26 UTC
- 편집된 시간: 2023년 2월 14일, 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPivateCAReadOnly

설명: AWS 사설 인증 기관에 대한 읽기 전용 액세스를 제공합니다.

AWSPivateCAReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPivateCAReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:30 UTC
- 편집된 시간: 2023년 2월 14일, 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPivateCAReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPriateCAUser

설명: 인증서 사용자에게 AWS 사설 인증 기관에 대한 액세스 권한을 제공합니다.

AWSPriateCAUser [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPriateCAUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:16 UTC
- 편집된 시간: 2023년 2월 14일, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPrivateMarketplaceAdminFullAccess

설명: AWS Private Marketplace의 모든 관리 작업에 대한 전체 액세스 권한을 제공합니다.

AWSPrivateMarketplaceAdminFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSPrivateMarketplaceAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 16:32 UTC
- 편집 시간: 2024년 2월 14일 22:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPrivateMarketplaceRequests

설명: AWS 프라이빗 마켓플레이스에서 요청을 생성할 수 있는 액세스 권한을 제공합니다.

AWSPrivateMarketplaceRequests [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivatemarketplaceRequests`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 28일, 21:44 UTC
- 편집된 시간: 2019년 10월 28일, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivatemarketplaceRequests`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPrivateNetworksServiceRolePolicy

설명: AWS 사설 네트워크 서비스가 고객을 대신하여 리소스를 관리할 수 있도록 합니다.

AWSPrivateNetworksServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 12월 16일, 23:17 UTC
- 편집된 시간: 2021년 12월 16일, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Action" : [
  "cloudwatch:PutMetricData"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "cloudwatch:namespace" : "AWS/Private5G"
  }
}
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonCodeBuildProvisioningBasicAccess

설명: AWS Proton CodeBuild 프로비저닝을 위한 빌드를 실행하려면 권한이 CodeBuild 필요합니다.

AWSProtonCodeBuildProvisioningBasicAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonCodeBuildProvisioningBasicAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 9일, 21:04 UTC
- 편집된 시간: 2022년 11월 9일, 21:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

설명: AWS Proton이 사용자를 대신하여 CodeBuild 및 기타 AWS 서비스를 사용하여 Proton 리소스 프로비저닝을 관리할 수 있도록 합니다.

AWSProtonCodeBuildProvisioningServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 9일, 21:32 UTC
- 편집된 시간: 2023년 5월 17일, 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonDeveloperAccess

설명: AWS Proton API 및 관리 콘솔에 대한 액세스를 제공하지만 Proton 템플릿 또는 환경의 관리는 허용하지 않습니다.

AWSProtonDeveloperAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonDeveloperAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:02 UTC
- 편집 시간: 2024년 6월 6일 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonFullAccess

설명: AWS Proton API 및 관리 콘솔에 대한 전체 액세스 권한을 제공합니다. 이러한 권한 외에도 S3 버킷에서 템플릿 번들을 등록하려면 Amazon S3에 대한 액세스가 필요하며, Proton의 서비스 역할을 생성하고 관리하려면 Amazon IAM에 대한 액세스도 필요합니다.

AWSProtonFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:07 UTC
- 편집 시간: 2024년 6월 6일 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonReadOnlyAccess

설명: AWS Proton API 및 관리 콘솔에 대한 읽기 전용 액세스를 제공합니다.

AWSProtonReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:09 UTC
- 편집된 시간: 2022년 11월 18일, 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonServiceGitSyncServiceRolePolicy

설명: AWS Proton이 git 저장소의 서비스, 환경 및 구성 요소 정의를 Proton으로 동기화할 수 있도록 하는 정책입니다. AWS

AWSProtonServiceGitSyncServiceRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 4일, 15:55 UTC
- 편집된 시간: 2023년 4월 4일, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSProtonSyncServiceRolePolicy

설명: Proton이 git 리포지토리 AWS 콘텐츠를 Proton에 동기화하거나 Proton 콘텐츠를 git 리포지토리에 동기화할 수 있도록 하는 정책입니다.

AWSProtonSyncServiceRolePolicy [관리형AWS 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 23일, 21:14 UTC
- 편집 시간: 2024년 5월 5일 01:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSPurchaseOrdersServiceRolePolicy

설명: 결제 콘솔에서 구매 주문을 보고 수정할 수 있는 권한을 부여합니다.

AWSPurchaseOrdersServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPurchaseOrdersServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 6일, 18:15 UTC
- 편집된 시간: 2023년 7월 17일, 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightAssetBundleExportPolicy

설명: QuickSight 에셋 번들 익스포트 작업을 수행하는 데 필요한 권한 세트를 제공합니다.

AWSQuickSightAssetBundleExportPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightAssetBundleExportPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 3월 27일 21:31 UTC
- 편집 시간: 2024년 3월 27일 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightAssetBundleImportPolicy

설명: QuickSight 에셋 번들 임포트 작업을 수행하는 데 필요한 권한 세트를 제공합니다.

AWSQuickSightAssetBundleImportPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightAssetBundleImportPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 3월 27일 21:40 UTC
- 편집 시간: 2024년 3월 27일 21:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*:*:vpccConnection/*"
},
{
  "Sid" : "AssetBundleImportOperations",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeAssetBundleImportJob",
    "quicksight:ListAssetBundleImportJobs",
    "quicksight:StartAssetBundleImportJob"
  ],
  "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
}
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuicksightAthenaAccess

설명: Athena 쿼리 결과에 사용되는 Athena API 및 S3 버킷에 대한 쿼사이트 액세스

AWSQuicksightAthenaAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSQuicksightAthenaAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 9일, 02:31 UTC
- 편집된 시간: 2021년 7월 7일, 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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



```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightDescribeRDS

설명: RDS QuickSight 리소스를 설명할 수 있습니다.

AWSQuickSightDescribeRDS [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightDescribeRDS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:24 UTC
- 편집된 시간: 2015년 11월 10일, 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightDescribeRedshift

설명: QuickSight Redshift 리소스를 설명할 수 있습니다.

AWSQuickSightDescribeRedshift [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightDescribeRedshift를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:25 UTC
- 편집된 시간: 2015년 11월 10일, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightElasticsearchPolicy

설명: 아마존에서 아마존 엘라스틱서치 리소스에 대한 액세스를 제공합니다. QuickSight

AWSQuickSightElasticsearchPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightElasticsearchPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 9월 9일, 17:27 UTC
- 편집된 시간: 2021년 9월 7일, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightIoTAnalyticsAccess

설명: IoT Analytics QuickSight 데이터세트에 대한 읽기 전용 액세스 권한 부여

AWSQuickSightIoTAnalyticsAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightIoTAnalyticsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 17:00 UTC
- 편집된 시간: 2017년 11월 29일, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightListIAM

설명: IAM QuickSight 엔티티를 나열할 수 있습니다.

AWSQuickSightListIAM [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightListIAM를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:25 UTC
- 편집된 시간: 2015년 11월 10일, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuicksightOpenSearchPolicy

설명: Amazon에서 Amazon OpenSearch 리소스에 대한 액세스를 제공합니다. QuickSight

AWSQuicksightOpenSearchPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuicksightOpenSearchPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 9월 7일, 23:26 UTC
- 편집된 시간: 2021년 9월 7일, 23:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightSageMakerPolicy

설명: Amazon에서 Amazon SageMaker 리소스에 대한 액세스를 제공합니다. QuickSight AWSQuickSightSageMakerPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightSageMakerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 1월 17일, 17:18 UTC
- 편집된 시간: 2023년 10월 30일, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
```

```

    "sagemaker:CreateTransformJob"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
},
{
  "Sid" : "SageMakerModelReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListModel",
    "sagemaker:DescribeModel"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3ObjectReadAccess",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : [
    "arn:aws:s3::quicksight-ml.*",
    "arn:aws:s3::sagemaker*"
  ]
},
{
  "Sid" : "S3ObjectUpdateAccess",
  "Effect" : "Allow",
  "Action" : "s3:PutObject",
  "Resource" : "arn:aws:s3::sagemaker*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "S3BucketReadAccess",
  "Effect" : "Allow",
  "Action" : "s3:ListBucket",
  "Resource" : "arn:aws:s3::sagemaker*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSQuickSightTimestreamPolicy

설명: AWS 타임스트림 API에 대한 AWS QuickSight 액세스. 고객은 이 정책을 AWS QuickSight 역할에 연결하여 데이터 및 메타데이터 검색을 허용할 수 있습니다.

AWSQuickSightTimestreamPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightTimestreamPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2020년 9월 30일, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSReachabilityAnalyzerServiceRolePolicy

설명: VPC Reachability Analyzer가 사용자를 대신하여 리소스에 AWS 액세스하고 조직과 통합할 수 있도록 합니다. AWS

AWSReachabilityAnalyzerServiceRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 23일, 17:12 UTC
- 편집 시간: 2024년 5월 15일 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRefactoringToolkitFullAccess

설명: 이 정책은 Microsoft Visual Studio용 .NET 리팩토링용 AWS 툴킷 확장 프로그램과 함께 AWS 서비스를 사용할 수 있는 권한을 부여합니다. 로컬 프로필에 첨부하기 위한 것입니다. AWS 이 정책은 Amazon S3에 애플리케이션 아티팩트를 업로드하고 Amazon S3에서 결과 아티팩트를 다운로드할 수

있도록 허용합니다. Amazon Elastic Container Registry (Amazon ECR) 를 사용하여 이미지를 저장 AWS CodeBuild 및 검색하고 이를 통해 컨테이너 이미지로 애플리케이션을 구축할 수 있습니다. 또한 Amazon Elastic Container Service (Amazon ECS) 와 AWS 같은 컨테이너 서비스에 애플리케이션을 배포하고, VPC 리소스를 선택적으로 생성하고, Directory Service와 같은 기존 인프라에 선택적으로 연결하고, 기타 관련 AWS 서비스를 사용할 수 있습니다.

AWSRefactoringToolkitFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSRefactoringToolkitFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 10월 25일, 16:41 UTC
- 편집 시간: 2024년 3월 25일 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRefactoringToolkitSidecarPolicy

설명: 이 정책은 Microsoft Visual Studio용 .NET 리팩토링용 AWS 툴킷 확장 프로그램을 AWS 사용하여 애플리케이션을 테스트하기 위해 만든 Amazon ECS 태스크에서 사용하기 위한 것입니다. 이 정책은 Amazon S3에서 애플리케이션 아티팩트를 다운로드하고, AWS Systems Manager를 사용하여 작업 상태를 전달하고, 기타 필수 서비스에 액세스할 수 있는 액세스 권한을 부여합니다.

AWSRefactoringToolkitSidecarPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSRefactoringToolkitSidecarPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 10월 25일, 16:41 UTC
- 편집된 시간: 2022년 10월 29일, 22:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSrePostPrivateCloudWatchAccess

설명: 지표 데이터를 게시할 수 있는 re:Post 비공개 액세스 권한을 제공합니다. CloudWatch

AWSrePostPrivateCloudWatchAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 15일, 16:37 UTC
- 편집된 시간: 2023년 11월 15일, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRepostSpaceSupportOperationsPolicy

설명: 이 정책을 통해 re:Post Space 서비스는 Space 응용 프로그램을 통해 생성된 지원 사례를 생성, 관리 및 해결할 수 있습니다.

AWSRepostSpaceSupportOperationsPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSRepostSpaceSupportOperationsPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 26일 21:52 UTC
- 편집 시간: 2023년 11월 26일, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResilienceHubAssessmentExecutionPolicy

설명: 평가를 실행하기 위해 다른 서비스에 대한 액세스를 허용하는 AWS Resilience Hub AWS 서비스 역할에 대한 정책입니다.

AWSResilienceHubAssessmentExecutionPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResilienceHubAssessmentExecutionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 12:32 UTC
- 편집 시간: 2024년 3월 24일 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceAccessManagerFullAccess

설명: AWS Resource Access Manager에 대한 전체 액세스 권한을 제공합니다.

AWSResourceAccessManagerFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceAccessManagerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 4일, 17:28 UTC
- 편집된 시간: 2019년 6월 4일, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceAccessManagerReadOnlyAccess

설명: AWS Resource Access Manager에 대한 읽기 전용 액세스 권한을 제공합니다.

AWSResourceAccessManagerReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceAccessManagerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 9일, 20:58 UTC
- 편집된 시간: 2019년 12월 9일, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceAccessManagerResourceShareParticipantAccess

설명: AWS 리소스 공유 참여자가 필요로 하는 Resource Access Manager API에 대한 액세스를 제공합니다.

AWSResourceAccessManagerResourceShareParticipantAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceAccessManagerResourceShareParticipantAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 12월 9일, 20:41 UTC
- 편집된 시간: 2019년 12월 9일, 20:41 UTC
- ARN: arn:aws:iam::aws:policy/
AWSResourceAccessManagerResourceShareParticipantAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceAccessManagerServiceRolePolicy

설명: 고객의 Organizations 구조에 대한 읽기 전용 AWS Resource Access Manager 액세스를 포함하는 정책입니다. 또한 역할을 자체 삭제할 수 있는 IAM 권한도 포함합니다.

AWSResourceAccessManagerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 19:28 UTC
- 편집된 시간: 2018년 11월 14일, 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceExplorerFullAccess

설명: 이 정책은 Resource Explorer 리소스에 액세스할 수 있는 관리자 권한을 부여하고 이러한 액세스를 지원하는 다른 AWS 서비스에 읽기 전용 권한을 부여합니다.

AWSResourceExplorerFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceExplorerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 7일, 20:01 UTC
- 편집된 시간: 2023년 11월 14일, 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceExplorerOrganizationsAccess

설명: 이 정책은 Resource Explorer에 관리자 권한을 부여하고 다른 AWS 서비스에는 이러한 액세스를 지원하는 읽기 전용 권한을 부여합니다. AWS Organizations 관리자는 콘솔에서 다중 계정 검색을 설정하고 관리하려면 이러한 권한이 필요합니다.

AWSResourceExplorerOrganizationsAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceExplorerOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 14일, 17:01 UTC
- 편집된 시간: 2023년 11월 14일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceExplorerReadOnlyAccess

설명: 이 정책은 Resource Explorer 리소스를 검색하고 볼 수 있는 읽기 전용 권한을 부여하고 이러한 액세스를 지원하는 다른 AWS 서비스에는 읽기 전용 권한을 부여합니다.

AWSResourceExplorerReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceExplorerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 7일, 19:56 UTC
- 편집된 시간: 2023년 11월 14일, 16:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceExplorerServiceRolePolicy

설명: Resource Explorer에서 사용자 대신 리소스 및 CloudTrail 이벤트를 보고 검색할 리소스를 인덱싱할 수 있도록 합니다.

AWSResourceExplorerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 10월 25일, 20:35 UTC
- 편집 시간: 2023년 12월 20일 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*:*/restapis",
        "arn:aws:apigateway:*:*/restapis/*/deployments"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
```

```
"amplify:ListDomainAssociations",
"amplifyuibuilder:ListComponents",
"amplifyuibuilder:ListThemes",
"app-integrations:ListEventIntegrations",
"apprunner:ListServices",
"apprunner:ListVpcConnectors",
"appstream:DescribeAppBlocks",
"appstream:DescribeApplications",
"appstream:DescribeFleets",
"appstream:DescribeImageBuilders",
"appstream:DescribeStacks",
"appsync:ListGraphQLApis",
"aps:ListRuleGroupsNamespaces",
"aps:ListWorkspaces",
"athena:ListDataCatalogs",
"athena:ListWorkGroups",
"autoscaling:DescribeAutoScalingGroups",
"backup:ListBackupPlans",
"backup:ListReportPlans",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:ListSchedulingPolicies",
"cloudformation:ListStacks",
"cloudformation:ListStackSets",
"cloudfront:ListCachePolicies",
"cloudfront:ListCloudFrontOriginAccessIdentities",
"cloudfront:ListDistributions",
"cloudfront:ListFieldLevelEncryptionConfigs",
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListOriginRequestPolicies",
"cloudfront:ListRealtimeLogConfigs",
"cloudfront:ListResponseHeadersPolicies",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"codeartifact:ListDomains",
"codeartifact:ListRepositories",
"codebuild:ListProjects",
"codecommit:ListRepositories",
"codeguru-profiler:ListProfilingGroups",
```

```
"codepipeline:ListPipelines",
"codestar-connections:ListConnections",
"cognito-identity:ListIdentityPools",
"cognito-idp:ListUserPools",
"databrew:ListDatasets",
"databrew:ListRecipes",
"databrew:ListRulesets",
"detective:ListGraphs",
"ds:DescribeDirectories",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeCapacityReservationFleets",
"ec2:DescribeCapacityReservations",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeElasticGpus",
"ec2:DescribeExportImageTasks",
"ec2:DescribeExportTasks",
"ec2:DescribeFleets",
"ec2:DescribeFlowLogs",
"ec2:DescribeFpgaImages",
"ec2:DescribeHostReservations",
"ec2:DescribeHosts",
"ec2:DescribeImages",
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstanceEventWindows",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeIpamPools",
"ec2:DescribeIpams",
"ec2:DescribeIpamScopes",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInsightsAccessScopeAnalyses",
"ec2:DescribeNetworkInsightsAccessScopes",
"ec2:DescribeNetworkInsightsAnalyses",
```

```
"ec2:DescribeNetworkInsightsPaths",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeReservedInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeSubnets",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPolicyTables",
"ec2:DescribeTransitGatewayRouteTableAnnouncements",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeVerifiedAccessEndpoints",
"ec2:DescribeVerifiedAccessGroups",
"ec2:DescribeVerifiedAccessInstances",
"ec2:DescribeVerifiedAccessTrustProviders",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetSubnetCidrReservations",
"ecr:DescribeRepositories",
"ecr-public:DescribeRepositories",
"ecs:DescribeCapacityProviders",
"ecs:DescribeServices",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:ListServices",
"ecs:ListTaskDefinitions",
"ecs:ListTasks",
"elasticache:DescribeCacheClusters",
```



```
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeReservedCacheNodes",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"emr-serverless:ListApplications",
"es:ListDomainNames",
"events:ListEventBuses",
"events:ListRules",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"finSPACE:ListEnvironments",
"firehose:ListDeliveryStreams",
"fis:ListExperimentTemplates",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"frauddetector:GetEntityTypeTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetLabels",
"frauddetector:GetOutcomes",
"frauddetector:GetVariables",
"gamelift:ListAliases",
"geo:ListPlaceIndexes",
"geo:ListTrackers",
"greengrass:ListComponents",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
```

```
"glue:GetDatabases",
"glue:GetJobs",
"glue:GetTables",
"glue:GetTriggers",
"greengrass:ListComponentVersions",
"greengrass:ListGroups",
"healthlake:ListFHIRDatastores",
"iam:ListGroups",
"iam:ListInstanceProfiles",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iot:ListJobTemplates",
"iot:ListAuthorizers",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListSecurityProfiles",
"iot:ListThings",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
```

```
"iotsitewise:ListGateways",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListWorkspaces",
"kafka:ListConfigurations",
"kms:ListKeys",
"ivs:ListChannels",
"ivs:ListStreamKeys",
"kafka:ListClusters",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisvideo:ListStreams",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lex:ListBots",
"lex:ListBotAliases",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"lookoutmetrics:ListAlerts",
"lookoutvision:ListProjects",
"mediapackage:ListChannels",
"mediapackage:ListOriginEndpoints",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mq:ListBrokers",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeACLs",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeUsers",
"mobiletargeting:GetApps",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTemplates",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetDevices",
```

```
"networkmanager:GetLinks",
"networkmanager:ListAttachments",
"networkmanager:ListCoreNetworks",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:ListAccounts",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListDelegatedAdministrators",
"panorama:ListPackages",
"personalize:ListDatasetGroups",
"personalize:ListDatasets",
"personalize:ListSchemas",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeReservedDBInstances",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
```

```
"rekognition:DescribeProjects",
"resiliencyhub:ListApps",
"resiliencyhub:ListResiliencyPolicies",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListViews",
"resource-groups:ListGroups",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverRules",
"s3:GetBucketLocation",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListStorageLensConfigurations",
"sagemaker:ListModels",
"sagemaker:ListNotebookInstances",
"secretsmanager:ListSecrets",
"servicecatalog:ListApplications",
"servicecatalog:ListAttributeGroups",
"signer:ListSigningProfiles",
"sns:ListTopics",
"sqs:ListQueues",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeInstanceInformation",
"ssm:DescribeMaintenanceWindows",
"ssm:DescribeMaintenanceWindowTargets",
"ssm:DescribeMaintenanceWindowTasks",
"ssm:DescribeParameters",
"ssm:DescribePatchBaselines",
"ssm-incidents:ListResponsePlans",
"ssm:ListAssociations",
"ssm:ListDocuments",
"ssm:ListInventoryEntries",
"ssm:ListResourceDataSync",
"states:ListActivities",
"states:ListStateMachines",
"timestream:ListDatabases",
"wisdom:listAssistantAssociations",
```

```
        "wisdom:ListAssistants",
        "wisdom:listKnowledgeBases"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSResourceGroupsReadOnlyAccess

설명: AWS Resource Groups의 읽기 전용 정책입니다.

AWSResourceGroupsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceGroupsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 10:27 UTC
- 편집된 시간: 2019년 2월 5일, 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRoboMaker_FullAccess

설명: AWS Management Console 및 SDK를 AWS RoboMaker 통해 전체 액세스 권한을 제공합니다. 또한 관련 서비스(예: S3, IAM)에 대한 선택적 액세스를 제공합니다.

AWSRoboMaker_FullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSRoboMaker_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 10일, 18:34 UTC
- 편집된 시간: 2021년 9월 16일, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRoboMakerReadOnlyAccess

설명: AWS Management Console 및 AWS RoboMaker SDK를 통해 읽기 전용 액세스를 제공합니다.

AWSRoboMakerReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSRoboMakerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 26일, 05:30 UTC

- 편집된 시간: 2020년 8월 28일, 23:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRoboMakerServicePolicy

설명: RoboMaker 서비스 정책

AWSRoboMakerServicePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 06:30 UTC
- 편집된 시간: 2021년 11월 11일, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRoboMakerServiceRolePolicy

설명: RoboMaker 서비스 정책

AWSRoboMakerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSRoboMakerServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 26일, 05:33 UTC
- 편집된 시간: 2018년 11월 26일, 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  }
}
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSRolesAnywhereServicePolicy

설명: IAM Roles Anywhere가 사용자 대신 사설 인증 기관에 서비스/사용 지표를 CloudWatch 게시하고 상태를 확인할 수 있도록 허용합니다.

AWSRolesAnywhereServicePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 5일, 15:26 UTC
- 편집된 시간: 2022년 7월 5일, 15:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSS3OnOutpostsServiceRolePolicy

설명: Amazon S3 on Outposts 서비스가 사용자를 대신하여 EC2 네트워크 리소스를 관리하도록 허용 하십시오.

AWSS3OnOutpostsServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 10월 3일, 20:32 UTC
- 편집된 시간: 2023년 10월 3일, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSavingsPlansFullAccess

설명: Savings Plans 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSSavingsPlansFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSSavingsPlansFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 6일, 22:45 UTC
- 편집된 시간: 2019년 11월 6일, 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSavingsPlansReadOnlyAccess

설명: Savings Plans 서비스에 대한 읽기 전용 액세스를 제공합니다.

AWSSavingsPlansReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSavingsPlansReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 6일, 22:45 UTC
- 편집된 시간: 2019년 11월 6일, 22:45 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSecurityHubFullAccess

설명: AWS Security Hub를 사용할 수 있는 전체 액세스 권한을 제공합니다.

AWSSecurityHubFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSecurityHubFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 23:54 UTC
- 편집 시간: 2024년 4월 23일 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSecurityHubOrganizationsAccess

설명: 조직 내에서 AWS Security Hub를 활성화하고 관리할 권한을 부여합니다. 조직 전체에서 서비스를 활성화하고 서비스에 대한 위임된 관리자 계정을 결정하는 작업이 포함됩니다.

AWSSecurityHubOrganizationsAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSecurityHubOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 15일, 20:53 UTC
- 편집 시간: 2023년 11월 16일 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSecurityHubReadOnlyAccess

설명: AWS Security Hub 리소스에 대한 읽기 전용 액세스를 제공합니다.

AWSSecurityHubReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSecurityHubReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 01:34 UTC
- 편집 시간: 2024년 2월 22일 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSecurityHubServiceRolePolicy

설명: AWS Security Hub가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다.

AWSSecurityHubServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 27일, 23:47 UTC
- 편집 시간: 2023년 11월 27일 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogAdminFullAccess

설명: 서비스 카탈로그 관리 기능에 대한 전체 액세스 권한을 제공합니다.

AWSServiceCatalogAdminFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 15일, 17:19 UTC

- 편집된 시간: 2023년 4월 13일, 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogAdminReadOnlyAccess

설명: Service Catalog 관리 기능에 대한 읽기 전용 액세스를 제공합니다.

AWSServiceCatalogAdminReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAdminReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 25일, 18:53 UTC
- 편집된 시간: 2019년 10월 25일, 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"

```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogAppRegistryFullAccess

설명: Service Catalog 앱 레지스트리 기능에 대한 전체 액세스 권한을 제공합니다.

AWSServiceCatalogAppRegistryFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAppRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 12일, 22:25 UTC
- 편집 시간: 2023년 12월 7일 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

설명: Service Catalog 애플리케이션 레지스트리 기능에 대한 읽기 전용 액세스를 제공합니다.

AWSServiceCatalogAppRegistryReadOnlyAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAppRegistryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 12일, 22:34 UTC
- 편집된 시간: 2022년 11월 17일, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

설명: Service AppRegistry Catalog가 사용자를 대신하여 리소스 그룹을 관리할 수 있도록 합니다.

AWSServiceCatalogAppRegistryServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 18일, 22:18 UTC
- 편집된 시간: 2022년 10월 26일, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogEndUserFullAccess

설명: 서비스 카탈로그 최종 사용자 기능에 대한 전체 액세스 권한을 제공합니다.

AWSServiceCatalogEndUserFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogEndUserFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 15일, 17:22 UTC
- 편집된 시간: 2019년 7월 10일, 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogEndUserReadOnlyAccess

설명: Service Catalog 최종 사용자 기능에 대한 읽기 전용 액세스를 제공합니다.

AWSServiceCatalogEndUserReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogEndUserReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 25일, 18:49 UTC
- 편집된 시간: 2019년 10월 25일, 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}

```



```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

설명: Organizations AWS 조직 구조와 AWS ServiceCatalog 동기화하기 위한 서비스 연결 역할 정책

AWSServiceCatalogOrgsDataSyncServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 10일, 20:48 UTC
- 편집된 시간: 2023년 4월 10일, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceCatalogSyncServiceRolePolicy

설명: 소스 리포지토리의 프로비저닝 아티팩트를 AWS ServiceCatalog 동기화하기 위한 서비스 연결 역할

AWSServiceCatalogSyncServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 15일, 21:20 UTC
- 편집 시간: 2024년 5월 3일 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForAmazonEKSNodegroup

설명: 고객 계정의 노드 그룹을 관리하는 데 필요한 권한입니다. 이러한 정책은 다음 리소스의 관리와 관련이 있습니다: AutoscalingGroups SecurityGroups, LaunchTemplates 및 InstanceProfiles

AWSServiceRoleForAmazonEKSNodegroup [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 7일, 01:34 UTC
- 편집 시간: 2024년 1월 4일 20:37 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSServiceRoleForAmazonEKSNodegroup

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForAmazonQDeveloper

설명: 이 서비스 연결 역할은 Amazon Q 개발자가 사용 정보를 제공할 수 있는 기능을 제공합니다.

AWSServiceRoleForAmazonQDeveloper [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 4월 25일 07:40 UTC
- 편집 시간: 2024년 4월 25일 07:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

설명: 경보에 사용되는 Systems Manager 리소스에 대한 액세스를 제공합니다. CloudWatch

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 10월 1일, 09:49 UTC
- 편집된 시간: 2020년 10월 1일, 09:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

설명: 사용자 대신 CloudWatch RDS Performance Insights 지표에 액세스할 수 있습니다.

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 9월 7일, 09:32 UTC
- 편집된 시간: 2023년 9월 7일, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "pi:GetResourceMetrics"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForCodeGuru-Profiler

설명: Amazon CodeGuru Profiler가 사용자를 대신하여 알림을 보내려면 서비스 연결 역할이 필요합니다.

AWSServiceRoleForCodeGuru-Profiler [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 26일, 22:04 UTC
- 편집된 시간: 2020년 6월 26일, 22:04 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForCodeWhispererPolicy

설명: 이 역할은 청구 계산을 CodeWhisperer 위해 계정의 데이터에 액세스할 수 있는 권한을 부여하고, Amazon에서 보안 보고서를 생성 및 액세스하고 CodeGuru, Amazon에 데이터를 내보낼 CloudWatch 수 있는 권한을 부여합니다.

AWSServiceRoleForCodeWhispererPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 24일, 19:39 UTC
- 편집 시간: 2024년 3월 29일 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForEC2ScheduledInstances

설명: EC2 정기 인스턴스에서 스팟 인스턴스를 시작하고 관리할 수 있습니다.

AWSServiceRoleForEC2ScheduledInstances [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 12일, 18:31 UTC
- 편집된 시간: 2017년 10월 12일, 18:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

설명: 이 서비스 연결 역할을 AWS GroundStation 사용하여 EC2를 호출하여 퍼블릭 IPv4 주소를 찾습니다.

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 12월 13일, 23:52 UTC
- 편집된 시간: 2022년 12월 13일, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForImageBuilder

설명: EC2가 사용자를 대신하여 AWS 서비스를 ImageBuilder 호출할 수 있도록 허용합니다.

AWSServiceRoleForImageBuilder [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 29일, 22:02 UTC
- 편집된 시간: 2023년 10월 19일, 21:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

정책 버전

정책 버전: v19(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn",
        "vmie.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:StartInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:CreateImage",
    "ec2:CreateLaunchTemplate",
    "ec2:DeregisterImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypeOfferings",
```

```
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:ModifyImageAttribute",
    "ec2:DescribeImportImageTasks",
    "ec2:DescribeExportImageTasks",
    "ec2:DescribeSnapshots",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateImage"
      ],
      "aws:RequestTag/CreatedBy" : [
        "EC2 Image Builder",
        "EC2 Fast Launch"
      ]
    }
  }
},
{
  "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:export-image-task/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : [
          "EC2 Image Builder",
          "EC2 Fast Launch"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:UpdateLicenseSpecificationsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListCommands",

```



```

    "ssm:ListCommandInvocations",
    "ssm:AddTagsToResource",
    "ssm:DescribeInstanceInformation",
    "ssm:GetAutomationExecution",
    "ssm:StopAutomationExecution",
    "ssm:ListInventoryEntries",
    "ssm:SendAutomationSignal",
    "ssm:DescribeInstanceAssociationsStatus",
    "ssm:DescribeAssociationExecutions",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
    "arn:aws:ssm:*:*:document/AWS-RunShellScript",
    "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
    "arn:aws:s3::*:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/CreatedBy" : [
        "EC2 Image Builder"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ssm:StartAutomationExecution",
  "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm>DeleteAssociation"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:association/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncryptFrom",
    "kms:ReEncryptTo",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "kms:EncryptionContextKeys" : [
        "aws:ebs:id"
      ]
    },
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
```

```
        "ec2.*.amazonaws.com"
    ]
}
},
{
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
            "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
            "kms:ViaService" : [
                "ec2.*.amazonaws.com"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "sts:AssumeRole",
    "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
    ],
    "Resource" : "*"
},
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ExportImage"
  ],
  "Resource" : "arn:aws:ec2:*:*:image/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ExportImage"
  ],
  "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CancelExportTask"
  ],
  "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : [
      "iam:AWSServiceName" : [
        "ssm.amazonaws.com",
        "ec2fastlaunch.amazonaws.com"
      ]
    ]
  }
},
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:EnableFastLaunch"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "inspector2:ListCoverage",
    "inspector2:ListFindings"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:TagResource"
  ],
  "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
    }
  }
}
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchDeleteImage"
  ],
  "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
  "Condition" : {
    "StringEquals" : {
      "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/ImageBuilder-*"
  ]
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForIoTSiteWise

설명: AWS IoT가 게이트웨이와 쿼리 데이터를 프로비저닝 및 관리할 수 SiteWise 있도록 합니다. 정책에는 그룹에 배포하기 위한 필수 AWS Greengrass 권한, 서비스 접두사가 붙은 함수를 생성 및 업데이트

트하기 위한 AWS Lambda 권한, 데이터스토어에서 데이터를 쿼리하기 위한 IoT AWS Analytics 권한이 포함됩니다.

`AWSServiceRoleForIoTSiteWise` [관리형AWS 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 19:19 UTC
- 편집된 시간: 2023년 11월 13일, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```


자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForLogDeliveryPolicy

설명: Log Delivery 서비스가 사용자 대신 로그 대상을 호출하여 로그를 전달할 수 있도록 합니다.

AWSServiceRoleForLogDeliveryPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 4일, 17:31 UTC
- 편집된 시간: 2021년 7월 15일, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "firehose:PutRecord",
    "firehose:PutRecordBatch",
    "firehose:ListTagsForDeliveryStream"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/LogDeliveryEnabled" : "true"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForMonitronPolicy

설명: Amazon Monitron에 사용자 대신 AWS SSO 사용자 할당을 포함하여 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

AWSServiceRoleForMonitronPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 2일, 19:06 UTC
- 편집된 시간: 2022년 9월 29일, 20:38 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForNeptuneGraphPolicy

설명: Amazon Neptune의 운영 및 사용 지표와 로그를 게시할 수 있는 Cloudwatch 액세스 권한을 제공합니다.

AWSServiceRoleForNeptuneGraphPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2023년 11월 29일, 14:03 UTC
- 편집 시간: 2023년 11월 29일, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

설명: Private Marketplace 리소스를 설명 및 업데이트하고 AWS Organizations를 설명할 수 있는 권한을 제공합니다.

AWSServiceRoleForPrivateMarketplaceAdminPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 2월 14일 22:28 UTC
- 편집 시간: 2024년 2월 14일 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForSMS

설명: AWS 서비스 인스턴스를 EC2, S3 및 Cloudformation을 AWS 포함하여 마이그레이션하는 데 필요한 서비스 및 리소스에 대한 액세스를 제공합니다.

AWSServiceRoleForSMS [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 8월 6일, 18:39 UTC
- 편집된 시간: 2020년 10월 15일, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
            }
        }
    }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRoleForUserSubscriptions

설명: Identity Center 리소스에 대한 사용자 구독 서비스에 액세스하여 구독을 자동으로 업데이트합니다.

AWSServiceRoleForUserSubscriptions [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 4월 25일 16:14 UTC
- 편집 시간: 2024년 4월 25일 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRolePolicyForBackupReports

설명: 사용자를 대신하여 규정 준수 보고서를 생성할 수 있는 AWS Backup 권한을 제공합니다.

AWSServiceRolePolicyForBackupReports [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2021년 8월 19일, 21:16 UTC
- 편집된 시간: 2023년 3월 10일, 00:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSServiceRolePolicyForBackupRestoreTesting

설명: 이 정책에는 복원을 테스트하고 테스트 중에 생성된 리소스를 정리할 수 있는 권한이 포함되어 있습니다.

AWSServiceRolePolicyForBackupRestoreTesting [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 10일, 23:37 UTC
- 편집 시간: 2024년 2월 14일 22:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSShieldDRTAccessPolicy

설명: 심각도가 높은 이벤트 발생 시 AWS DDoS 공격 완화를 지원하기 위해 AWS 계정 위해 DDoS 대응팀에 제한된 액세스 권한을 제공합니다.

AWSShieldDRTAccessPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSShieldDRTAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 6월 5일, 22:29 UTC
- 편집된 시간: 2020년 12월 15일, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSShieldServiceRolePolicy

설명: AWS Shield가 사용자 대신 AWS 리소스에 액세스하여 DDoS 보호를 제공할 수 있도록 합니다.

AWSShieldServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 19:17 UTC
- 편집된 시간: 2021년 11월 17일, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
"Statement" : [
  {
    "Sid" : "AWSShield",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:GetWebACL",
      "wafv2:UpdateWebACL",
      "wafv2:GetWebACLForResource",
      "wafv2:ListResourcesForWebACL",
      "cloudfront:ListDistributions",
      "cloudfront:GetDistribution"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSMForSAPServiceLinkedRolePolicy

설명: AWS Systems Manager for SAP에 SAP 소프트웨어를 관리하고 통합하는 데 필요한 권한을 제공합니다 AWS.

AWSSSMForSAPServiceLinkedRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 16일, 01:18 UTC
- 편집 시간: 2024년 4월 11일 18:31 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSMOpsInsightsServiceRolePolicy

설명: 서비스 연결 역할 정책 AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 16일, 20:12 UTC
- 편집된 시간: 2021년 6월 16일, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSODirectoryAdministrator

설명: SSO 디렉터리에 대한 관리자 액세스

AWSSSODirectoryAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSODirectoryAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 31일, 23:54 UTC
- 편집된 시간: 2022년 10월 20일, 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSODirectoryReadOnly

설명: SSO 디렉터리 ReadOnly 액세스

AWSSSODirectoryReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSODirectoryReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 31일, 23:49 UTC
- 편집된 시간: 2022년 11월 16일, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSOMasterAccountAdministrator

설명: AWS Organizations의 마스터 및 멤버 계정과 클라우드 AWS 애플리케이션을 관리하기 위한 SSO 내 액세스를 제공합니다.

AWSSSOMasterAccountAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSOMasterAccountAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:36 UTC
- 편집 시간: 2024년 4월 26일 00:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{  
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSOMemberAccountAdministrator

설명: AWS Organizations 회원 계정 및 클라우드 애플리케이션을 관리하기 위한 AWS SSO 내 액세스를 제공합니다.

AWSSSOMemberAccountAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSOMemberAccountAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:45 UTC
- 편집 시간: 2024년 4월 26일 00:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSOREadOnly

설명: AWS SSO 구성에 대한 읽기 전용 액세스를 제공합니다.

AWSSSOREadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSOREadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:24 UTC
- 편집 시간: 2024년 4월 26일 00:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOREadOnly

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSSOServiceRolePolicy

설명: 사용자를 대신하여 IAM 역할, 정책 및 AWS SAML IdP를 비롯한 AWS 리소스를 관리할 수 있는 SSO 권한을 부여합니다.

AWSSSOServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 12월 5일, 18:36 UTC
- 편집된 시간: 2022년 10월 20일, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSS0ServiceRolePolicy`

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStepFunctionsConsoleFullAccess

설명: 콘솔에 대한 사용자/역할 등의 액세스를 제공하기 위한 액세스 정책입니다. AWS StepFunctions 완전한 콘솔 경험을 위해 사용자는 이 정책 외에도 서비스에서 위임할 수 있는 다른 IAM 역할에 대한 iam: PassRole 권한이 필요할 수 있습니다.

AWSStepFunctionsConsoleFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSStepFunctionsConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:54 UTC
- 편집된 시간: 2017년 1월 12일, 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStepFunctionsFullAccess

설명: API에 대한 사용자/역할 등의 액세스를 제공하기 위한 액세스 정책입니다. AWS StepFunctions 전체 액세스를 위해서는 이 정책 외에도 사용자에게 서비스가 위임할 수 있는 하나 이상의 IAM 역할에 대한 iam: PassRole 권한이 있어야 합니다.

AWSStepFunctionsFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSStepFunctionsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:51 UTC

- 편집된 시간: 2017년 1월 11일, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStepFunctionsReadOnlyAccess

설명: 사용자/역할 등에게 서비스에 대한 읽기 전용 액세스를 제공하기 위한 액세스 정책입니다. AWS StepFunctions

AWSStepFunctionsReadOnlyAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 `AWSStepFunctionsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:46 UTC
- 편집 시간: 2024년 4월 26일 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStorageGatewayFullAccess

설명: 를 통해 AWS Storage Gateway에 대한 전체 액세스를 제공합니다 AWS Management Console.

AWSStorageGatewayFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSStorageGatewayFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2022년 9월 6일, 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStorageGatewayReadOnlyAccess

설명: 를 통해 AWS Storage Gateway에 액세스할 수 AWS Management Console 있습니다.

AWSStorageGatewayReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSStorageGatewayReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2022년 9월 6일, 20:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSStorageGatewayServiceRolePolicy

설명: Storage Gateway에서 다른 서비스를 AWS Storage Gateway와 통합할 수 있도록 하는 데 사용하는 AWS 서비스 연결 역할입니다.

AWSStorageGatewayServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 2월 17일, 19:03 UTC
- 편집된 시간: 2021년 2월 17일, 19:03 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupplyChainFederationAdminAccess

설명: AWS 공급망 애플리케이션 내에서 작업을 수행하는 데 필요한 권한을 포함하여 AWS 공급망 연동 사용자에게 AWS 공급망 애플리케이션에 대한 액세스 권한을 AWSSupplyChainFederationAdminAccess 제공합니다. 이 정책은 IAM Identity Center 사용자 및 그룹에 대한 관리 권한을 제공하며 AWS 공급망이 사용자를 대신하여 생성한 역할에 연결됩니다. AWSSupplyChainFederationAdminAccess 정책을 다른 IAM 엔티티에 연결해서는 안 됩니다.

AWSSupplyChainFederationAdminAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupplyChainFederationAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 3월 1일, 18:54 UTC
- 편집된 시간: 2023년 11월 1일, 18:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportAccess

설명: 사용자가 AWS Support 센터에 액세스할 수 있습니다.

AWSSupportAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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


}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportAppFullAccess

설명: AWS Support 앱 및 기타 필수 서비스 (예: Service Quotas AWS Support) 에 대한 전체 액세스 권한을 제공합니다. 이 정책에는 사용자가 지원 사례를 AWS Support 문의하고, 서비스 할당량을 변경하고, 관련 서비스 연결 역할을 생성할 수 있도록 지원 서비스를 사용할 수 있는 권한이 포함됩니다.

AWSSupportAppFullAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportAppFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 22일, 16:53 UTC
- 편집된 시간: 2022년 8월 22일, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportAppReadOnlyAccess

설명: AWS Support 앱에 대한 읽기 전용 액세스를 제공합니다.

AWSSupportAppReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportAppReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 22일, 17:01 UTC
- 편집된 시간: 2022년 8월 22일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportPlansFullAccess

설명: 지원 계획에 대한 전체 액세스 권한을 제공합니다.

AWSSupportPlansFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportPlansFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 9월 27일, 18:19 UTC
- 편집된 시간: 2023년 5월 9일, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "supportplans:GetSupportPlan",
      "supportplans:GetSupportPlanUpdateStatus",
      "supportplans:StartSupportPlanUpdate",
      "supportplans:CreateSupportPlanSchedule"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportPlansReadOnlyAccess

설명: 지원 계획에 대한 읽기 전용 액세스를 제공합니다.

AWSSupportPlansReadOnlyAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportPlansReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 9월 27일, 18:08 UTC
- 편집된 시간: 2022년 9월 27일, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSupportServiceRolePolicy

설명: AWS Support AWS 리소스에 액세스하여 청구, 관리 및 지원 서비스를 제공할 수 있습니다.

AWSSupportServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 4월 19일, 18:04 UTC
- 편집 시간: 2024년 5월 2일 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

정책 버전

정책 버전: v36(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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",
"dms:getLifecyclePolicies",
"dms:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
```

```
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
"drs:describeJobLogItems",
"drs:describeJobs",
"drs:describeLaunchConfigurationTemplates",
"drs:describeRecoveryInstances",
"drs:describeRecoverySnapshots",
"drs:describeReplicationConfigurationTemplates",
"drs:describeSourceNetworks",
"drs:describeSourceServers",
"drs:getLaunchConfiguration",
"drs:getReplicationConfiguration",
"drs:listExtensibleSourceServers",
"drs:listLaunchActions",
"drs:listStagingAccounts",
"ds:describeClientAuthenticationSettings",
"ds:describeConditionalForwarders",
"ds:describeDirectories",
"ds:describeDomainControllers",
"ds:describeEventTopics",
"ds:describeLDAPSSettings",
"ds:describeSharedDirectories",
"ds:describeSnapshots",
"ds:describeTrusts",
```

```
"ds:getDirectoryLimits",
"ds:getSnapshotLimits",
"ds:listIpRoutes",
"ds:listSchemaExtensions",
"ds:listTagsForResource",
"dynamodb:describeBackup",
"dynamodb:describeContinuousBackups",
"dynamodb:describeContributorInsights",
"dynamodb:describeExport",
"dynamodb:describeGlobalTable",
"dynamodb:describeImport",
"dynamodb:describeKinesisStreamingDestination",
"dynamodb:describeLimits",
"dynamodb:describeStream",
"dynamodb:describeTable",
"dynamodb:describeTimeToLive",
"dynamodb:listBackups",
"dynamodb:listContributorInsights",
"dynamodb:listExports",
"dynamodb:listGlobalTables",
"dynamodb:listImports",
"dynamodb:listStreams",
"dynamodb:listTables",
"dynamodb:listTagsOfResource",
"ec2:describeAccountAttributes",
"ec2:describeAddresses",
"ec2:describeAddressesAttribute",
"ec2:describeAddressTransfers",
"ec2:describeAggregateIdFormat",
"ec2:describeAvailabilityZones",
"ec2:describeBundleTasks",
"ec2:describeByoipCidrs",
"ec2:describeCapacityReservationFleets",
"ec2:describeCapacityReservations",
"ec2:describeCarrierGateways",
"ec2:describeClassicLinkInstances",
"ec2:describeClientVpnAuthorizationRules",
"ec2:describeClientVpnConnections",
"ec2:describeClientVpnEndpoints",
"ec2:describeClientVpnRoutes",
"ec2:describeClientVpnTargetNetworks",
"ec2:describeCoipPools",
"ec2:describeConversionTasks",
"ec2:describeCustomerGateways",
```

```
"ec2:describeDhcpOptions",
"ec2:describeEgressOnlyInternetGateways",
"ec2:describeExportImageTasks",
"ec2:describeExportTasks",
"ec2:describeFastLaunchImages",
"ec2:describeFastSnapshotRestores",
"ec2:describeFleetHistory",
"ec2:describeFleetInstances",
"ec2:describeFleets",
"ec2:describeFlowLogs",
"ec2:describeFpgaImageAttribute",
"ec2:describeFpgaImages",
"ec2:describeHostReservationOfferings",
"ec2:describeHostReservations",
"ec2:describeHosts",
"ec2:describeIamInstanceProfileAssociations",
"ec2:describeIdentityIdFormat",
"ec2:describeIdFormat",
"ec2:describeImageAttribute",
"ec2:describeImages",
"ec2:describeImportImageTasks",
"ec2:describeImportSnapshotTasks",
"ec2:describeInstanceAttribute",
"ec2:describeInstanceCreditSpecifications",
"ec2:describeInstanceEventNotificationAttributes",
"ec2:describeInstanceEventWindows",
"ec2:describeInstances",
"ec2:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"ec2:describeIpams",
"ec2:describeIpamScopes",
"ec2:describeIpv6Pools",
"ec2:describeKeyPairs",
"ec2:describeLaunchTemplates",
"ec2:describeLaunchTemplateVersions",
"ec2:describeLocalGatewayRouteTables",
"ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:describeLocalGatewayRouteTableVpcAssociations",
"ec2:describeLocalGateways",
"ec2:describeLocalGatewayVirtualInterfaceGroups",
"ec2:describeLocalGatewayVirtualInterfaces",
```

```
"ec2:describeManagedPrefixLists",
"ec2:describeMovingAddresses",
"ec2:describeNatGateways",
"ec2:describeNetworkAcls",
"ec2:describeNetworkInterfaceAttribute",
"ec2:describeNetworkInterfaces",
"ec2:describePlacementGroups",
"ec2:describePrefixLists",
"ec2:describePrincipalIdFormat",
"ec2:describePublicIpv4Pools",
"ec2:describeRegions",
"ec2:describeReservedInstances",
"ec2:describeReservedInstancesListings",
"ec2:describeReservedInstancesModifications",
"ec2:describeReservedInstancesOfferings",
"ec2:describeRouteTables",
"ec2:describeScheduledInstanceAvailability",
"ec2:describeScheduledInstances",
"ec2:describeSecurityGroupReferences",
"ec2:describeSecurityGroupRules",
"ec2:describeSecurityGroups",
"ec2:describeSnapshotAttribute",
"ec2:describeSnapshots",
"ec2:describeSpotDatafeedSubscription",
"ec2:describeSpotFleetInstances",
"ec2:describeSpotFleetRequestHistory",
"ec2:describeSpotFleetRequests",
"ec2:describeSpotInstanceRequests",
"ec2:describeSpotPriceHistory",
"ec2:describeStaleSecurityGroups",
"ec2:describeStoreImageTasks",
"ec2:describeSubnets",
"ec2:describeTags",
"ec2:describeTrafficMirrorFilters",
"ec2:describeTrafficMirrorSessions",
"ec2:describeTrafficMirrorTargets",
"ec2:describeTransitGatewayAttachments",
"ec2:describeTransitGatewayConnectPeers",
"ec2:describeTransitGatewayMulticastDomains",
"ec2:describeTransitGatewayPeeringAttachments",
"ec2:describeTransitGatewayPolicyTables",
"ec2:describeTransitGatewayRouteTableAnnouncements",
"ec2:describeTransitGatewayRouteTables",
"ec2:describeTransitGateways",
```

```
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"ec2:describeVpcAttribute",
"ec2:describeVpcClassicLink",
"ec2:describeVpcClassicLinkDnsSupport",
"ec2:describeVpcEndpointConnectionNotifications",
"ec2:describeVpcEndpointConnections",
"ec2:describeVpcEndpoints",
"ec2:describeVpcEndpointServiceConfigurations",
"ec2:describeVpcEndpointServicePermissions",
"ec2:describeVpcEndpointServices",
"ec2:describeVpcPeeringConnections",
"ec2:describeVpcs",
"ec2:describeVpnConnections",
"ec2:describeVpnGateways",
"ec2:getAssociatedIpv6PoolCidrs",
"ec2:getCapacityReservationUsage",
"ec2:getCoipPoolUsage",
"ec2:getConsoleOutput",
"ec2:getConsoleScreenshot",
"ec2:getDefaultCreditSpecification",
"ec2:getEbsDefaultKmsKeyId",
"ec2:getEbsEncryptionByDefault",
"ec2:getGroupsForCapacityReservation",
"ec2:getHostReservationPurchasePreview",
"ec2:getInstanceTypesFromInstanceRequirements",
"ec2:getIpamAddressHistory",
"ec2:getIpamPoolAllocations",
"ec2:getIpamPoolCidrs",
"ec2:getIpamResourceCidrs",
"ec2:getLaunchTemplateData",
"ec2:getManagedPrefixListAssociations",
"ec2:getManagedPrefixListEntries",
"ec2:getReservedInstancesExchangeQuote",
"ec2:getSerialConsoleAccessStatus",
"ec2:getSpotPlacementScores",
"ec2:getTransitGatewayMulticastDomainAssociations",
```

```
"ec2:getTransitGatewayPrefixListReferences",
"ec2:getVerifiedAccessEndpointPolicy",
"ec2:getVerifiedAccessGroupPolicy",
"ec2:listImagesInRecycleBin",
"ec2:listSnapshotsInRecycleBin",
"ec2:searchLocalGatewayRoutes",
"ec2:searchTransitGatewayMulticastGroups",
"ec2:searchTransitGatewayRoutes",
"ecr-public:describeImages",
"ecr-public:describeImageTags",
"ecr-public:describeRegistries",
"ecr-public:describeRepositories",
"ecr-public:getRegistryCatalogData",
"ecr-public:getRepositoryCatalogData",
"ecr-public:getRepositoryPolicy",
"ecr-public:listTagsForResource",
"ecr:batchCheckLayerAvailability",
"ecr:batchGetRepositoryScanningConfiguration",
"ecr:describeImages",
"ecr:describeImageReplicationStatus",
"ecr:describeImageScanFindings",
"ecr:describePullThroughCacheRules",
"ecr:describeRegistry",
"ecr:describeRepositories",
"ecr:getLifecyclePolicy",
"ecr:getLifecyclePolicyPreview",
"ecr:getRegistryPolicy",
"ecr:getRegistryScanningConfiguration",
"ecr:getRepositoryPolicy",
"ecr:listImages",
"ecr:listTagsForResource",
"ecs:describeCapacityProviders",
"ecs:describeClusters",
"ecs:describeContainerInstances",
"ecs:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"ecs:getTaskProtection",
"ecs:listAccountSettings",
"ecs:listAttributes",
"ecs:listClusters",
"ecs:listContainerInstances",
"ecs:listServices",
```

```
"ecs:listServicesByNamespace",
"ecs:listTagsForResource",
"ecs:listTaskDefinitionFamilies",
"ecs:listTaskDefinitions",
"ecs:listTasks",
"eks:describeAccessEntry",
"eks:describeAddon",
"eks:describeAddonConfiguration",
"eks:describeAddonVersions",
"eks:describeCluster",
"eks:describeEksAnywhereSubscription",
"eks:describeFargateProfile",
"eks:describeIdentityProviderConfig",
"eks:describeNodegroup",
"eks:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"eks:listUpdates",
"elasticache:describeCacheClusters",
"elasticache:describeCacheEngineVersions",
"elasticache:describeCacheParameterGroups",
"elasticache:describeCacheParameters",
"elasticache:describeCacheSecurityGroups",
"elasticache:describeCacheSubnetGroups",
"elasticache:describeEngineDefaultParameters",
"elasticache:describeEvents",
"elasticache:describeGlobalReplicationGroups",
"elasticache:describeReplicationGroups",
"elasticache:describeReservedCacheNodes",
"elasticache:describeReservedCacheNodesOfferings",
"elasticache:describeServerlessCaches",
"elasticache:describeServerlessCacheSnapshots",
"elasticache:describeServiceUpdates",
"elasticache:describeSnapshots",
"elasticache:describeUpdateActions",
"elasticache:describeUserGroups",
"elasticache:describeUsers",
```



```
"elasticache:listAllowedNodeTypeModifications",
"elasticache:listTagsForResource",
"elasticbeanstalk:checkDNSAvailability",
"elasticbeanstalk:describeAccountAttributes",
"elasticbeanstalk:describeApplicationVersions",
"elasticbeanstalk:describeApplications",
"elasticbeanstalk:describeConfigurationOptions",
"elasticbeanstalk:describeEnvironmentHealth",
"elasticbeanstalk:describeEnvironmentManagedActionHistory",
"elasticbeanstalk:describeEnvironmentManagedActions",
"elasticbeanstalk:describeEnvironmentResources",
"elasticbeanstalk:describeEnvironments",
"elasticbeanstalk:describeEvents",
"elasticbeanstalk:describeInstancesHealth",
"elasticbeanstalk:describePlatformVersion",
"elasticbeanstalk:listAvailableSolutionStacks",
"elasticbeanstalk:listPlatformBranches",
"elasticbeanstalk:listPlatformVersions",
"elasticbeanstalk:validateConfigurationSettings",
"elasticfilesystem:describeAccessPoints",
"elasticfilesystem:describeFileSystemPolicy",
"elasticfilesystem:describeFileSystems",
"elasticfilesystem:describeLifecycleConfiguration",
"elasticfilesystem:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"elasticfilesystem:describeTags",
"elasticfilesystem:listTagsForResource",
"elasticloadbalancing:describeAccountLimits",
"elasticloadbalancing:describeInstanceHealth",
"elasticloadbalancing:describeListenerCertificates",
"elasticloadbalancing:describeListeners",
"elasticloadbalancing:describeLoadBalancerAttributes",
"elasticloadbalancing:describeLoadBalancerPolicies",
"elasticloadbalancing:describeLoadBalancerPolicyTypes",
"elasticloadbalancing:describeLoadBalancers",
"elasticloadbalancing:describeRules",
"elasticloadbalancing:describeSSLPolicies",
"elasticloadbalancing:describeTags",
"elasticloadbalancing:describeTargetGroupAttributes",
"elasticloadbalancing:describeTargetGroups",
"elasticloadbalancing:describeTargetHealth",
"elasticmapreduce:describeCluster",
"elasticmapreduce:describeNotebookExecution",
"elasticmapreduce:describeReleaseLabel",
```

```
"elasticmapreduce:describeSecurityConfiguration",
"elasticmapreduce:describeStep",
"elasticmapreduce:describeStudio",
"elasticmapreduce:getAutoTerminationPolicy",
"elasticmapreduce:getBlockPublicAccessConfiguration",
"elasticmapreduce:getManagedScalingPolicy",
"elasticmapreduce:getStudioSessionMapping",
"elasticmapreduce:listBootstrapActions",
"elasticmapreduce:listClusters",
"elasticmapreduce:listInstanceFleets",
"elasticmapreduce:listInstanceGroups",
"elasticmapreduce:listInstances",
"elasticmapreduce:listNotebookExecutions",
"elasticmapreduce:listReleaseLabels",
"elasticmapreduce:listSecurityConfigurations",
"elasticmapreduce:listSteps",
"elasticmapreduce:listStudios",
"elasticmapreduce:listStudioSessionMappings",
"elastictranscoder:listJobsByPipeline",
"elastictranscoder:listJobsByStatus",
"elastictranscoder:listPipelines",
"elastictranscoder:listPresets",
"elastictranscoder:readPipeline",
"elastictranscoder:readPreset",
"emr-containers:describeJobRun",
"emr-containers:describeJobTemplate",
"emr-containers:describeManagedEndpoint",
"emr-containers:describeVirtualCluster",
"emr-containers:listJobRuns",
"emr-containers:listJobTemplates",
"emr-containers:listManagedEndpoints",
"emr-containers:listVirtualClusters",
"emr-serverless:getApplication",
"emr-serverless:getJobRun",
"emr-serverless:listApplications",
"es:describeDomain",
"es:describeDomainAutoTunes",
"es:describeDomainChangeProgress",
"es:describeDomainConfig",
"es:describeDomains",
"es:describeDryRunProgress",
"es:describeElasticsearchDomain",
"es:describeElasticsearchDomainConfig",
"es:describeElasticsearchDomains",
```

```
"es:describeInboundConnections",
"es:describeInstanceTypeLimits",
"es:describeOutboundConnections",
"es:describePackages",
"es:describeReservedInstanceOfferings",
"es:describeReservedInstances",
"es:describeVpcEndpoints",
"es:getCompatibleVersions",
"es:getPackageVersionHistory",
"es:getUpgradeHistory",
"es:getUpgradeStatus",
"es:listDomainNames",
"es:listDomainsForPackage",
"es:listInstanceTypeDetails",
"es:listPackagesForDomain",
"es:listScheduledActions",
"es:listTags",
"es:listVersions",
"es:listVpcEndpointAccess",
"es:listVpcEndpoints",
"es:listVpcEndpointsForDomain",
"evidently:getExperiment",
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
```

```
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
"fms:listPolicies",
"forecast:describeDataset",
"forecast:describeDatasetGroup",
"forecast:describeDatasetImportJob",
"forecast:describeForecast",
"forecast:describeForecastExportJob",
"forecast:describePredictor",
"forecast:getAccuracyMetrics",
"forecast:listDatasetGroups",
"forecast:listDatasetImportJobs",
"forecast:listDatasets",
"forecast:listForecastExportJobs",
"forecast:listForecasts",
"forecast:listPredictors",
"fsx:describeBackups",
"fsx:describeDataRepositoryAssociations",
"fsx:describeDataRepositoryTasks",
"fsx:describeFileCaches",
"fsx:describeFileSystems",
"fsx:describeSnapshots",
"fsx:describeStorageVirtualMachines",
"fsx:describeVolumes",
"fsx:listTagsForResource",
"gamelift:describeAlias",
"gamelift:describeBuild",
```

```
"gamelift:describeEC2InstanceLimits",
"gamelift:describeFleetAttributes",
"gamelift:describeFleetCapacity",
"gamelift:describeFleetEvents",
"gamelift:describeFleetLocationAttributes",
"gamelift:describeFleetLocationCapacity",
"gamelift:describeFleetLocationUtilization",
"gamelift:describeFleetPortSettings",
"gamelift:describeFleetUtilization",
"gamelift:describeGameServer",
"gamelift:describeGameServerGroup",
"gamelift:describeGameSessionDetails",
"gamelift:describeGameSessionPlacement",
"gamelift:describeGameSessionQueues",
"gamelift:describeGameSessions",
"gamelift:describeInstances",
"gamelift:describeMatchmaking",
"gamelift:describeMatchmakingConfigurations",
"gamelift:describeMatchmakingRuleSets",
"gamelift:describePlayerSessions",
"gamelift:describeRuntimeConfiguration",
"gamelift:describeScalingPolicies",
"gamelift:describeScript",
"gamelift:listAliases",
"gamelift:listBuilds",
"gamelift:listFleets",
"gamelift:listGameServerGroups",
"gamelift:listGameServers",
"gamelift:listScripts",
"gamelift:resolveAlias",
"glacier:describeJob",
"glacier:describeVault",
"glacier:getDataRetrievalPolicy",
"glacier:getVaultAccessPolicy",
"glacier:getVaultLock",
"glacier:getVaultNotifications",
"glacier:listJobs",
"glacier:listTagsForVault",
"glacier:listVaults",
"globalaccelerator:describeAccelerator",
"globalaccelerator:describeAcceleratorAttributes",
"globalaccelerator:describeEndpointGroup",
"globalaccelerator:describeListener",
"globalaccelerator:listAccelerators",
```

```
"globalaccelerator:listEndpointGroups",
"globalaccelerator:listListeners",
"glue:batchGetBlueprints",
"glue:batchGetCrawlers",
"glue:batchGetDevEndpoints",
"glue:batchGetJobs",
"glue:batchGetPartition",
"glue:batchGetTriggers",
"glue:batchGetWorkflows",
"glue:checkSchemaVersionValidity",
"glue:getBlueprint",
"glue:getBlueprintRun",
"glue:getBlueprintRuns",
"glue:getCatalogImportStatus",
"glue:getClassifier",
"glue:getClassifiers",
"glue:getColumnStatisticsForPartition",
"glue:getColumnStatisticsForTable",
"glue:getCrawler",
"glue:getCrawlerMetrics",
"glue:getCrawlers",
"glue:getCustomEntityType",
"glue:getDatabase",
"glue:getDatabases",
"glue:getDataflowGraph",
"glue:getDataQualityResult",
"glue:getDataQualityRuleRecommendationRun",
"glue:getDataQualityRuleset",
"glue:getDataQualityRulesetEvaluationRun",
"glue:getDevEndpoint",
"glue:getDevEndpoints",
"glue:getJob",
"glue:getJobRun",
"glue:getJobRuns",
"glue:getJobs",
"glue:getMapping",
"glue:getMLTaskRun",
"glue:getMLTaskRuns",
"glue:getMLTransform",
"glue:getMLTransforms",
"glue:getPartition",
"glue:getPartitionIndexes",
"glue:getPartitions",
"glue:getRegistry",
```

```
"glue:getResourcePolicies",
"glue:getResourcePolicy",
"glue:getSchema",
"glue:getSchemaByDefinition",
"glue:getSchemaVersion",
"glue:getSchemaVersionsDiff",
"glue:getSession",
"glue:getStatement",
"glue:getTable",
"glue:getTables",
"glue:getTableVersions",
"glue:getTrigger",
"glue:getTriggers",
"glue:getUserDefinedFunction",
"glue:getUserDefinedFunctions",
"glue:getWorkflow",
"glue:getWorkflowRun",
"glue:getWorkflowRuns",
"glue:listCrawlers",
"glue:listCrawls",
"glue:listDataQualityResults",
"glue:listDataQualityRuleRecommendationRuns",
"glue:listDataQualityRulesetEvaluationRuns",
"glue:listDataQualityRulesets",
"glue:listDevEndpoints",
"glue:listMLTransforms",
"glue:listRegistries",
"glue:listSchemas",
"glue:listSchemaVersions",
"glue:listSessions",
"glue:listStatements",
"glue:querySchemaVersionMetadata",
"grafana:describeWorkspace",
"grafana:describeWorkspaceAuthentication",
"grafana:listPermissions",
"grafana:listVersions",
"grafana:listWorkspaces",
"greengrass:getConnectivityInfo",
"greengrass:getCoreDefinition",
"greengrass:getCoreDefinitionVersion",
"greengrass:getDeploymentStatus",
"greengrass:getDeviceDefinition",
"greengrass:getDeviceDefinitionVersion",
"greengrass:getFunctionDefinition",
```

```
"greengrass:getFunctionDefinitionVersion",
"greengrass:getGroup",
"greengrass:getGroupCertificateAuthority",
"greengrass:getGroupVersion",
"greengrass:getLoggerDefinition",
"greengrass:getLoggerDefinitionVersion",
"greengrass:getResourceDefinitionVersion",
"greengrass:getServiceRoleForAccount",
"greengrass:getSubscriptionDefinition",
"greengrass:getSubscriptionDefinitionVersion",
"greengrass:listCoreDefinitions",
"greengrass:listCoreDefinitionVersions",
"greengrass:listDeployments",
"greengrass:listDeviceDefinitions",
"greengrass:listDeviceDefinitionVersions",
"greengrass:listFunctionDefinitions",
"greengrass:listFunctionDefinitionVersions",
"greengrass:listGroups",
"greengrass:listGroupVersions",
"greengrass:listLoggerDefinitions",
"greengrass:listLoggerDefinitionVersions",
"greengrass:listResourceDefinitions",
"greengrass:listResourceDefinitionVersions",
"greengrass:listSubscriptionDefinitions",
"greengrass:listSubscriptionDefinitionVersions",
"guardduty:getDetector",
"guardduty:getFindings",
"guardduty:getFindingsStatistics",
"guardduty:getInvitationsCount",
"guardduty:getIPSet",
"guardduty:getMasterAccount",
"guardduty:getMembers",
"guardduty:getThreatIntelSet",
"guardduty:listDetectors",
"guardduty:listFindings",
"guardduty:listInvitations",
"guardduty:listIPSets",
"guardduty:listMembers",
"guardduty:listThreatIntelSets",
"health:describeAffectedAccountsForOrganization",
"health:describeAffectedEntities",
"health:describeAffectedEntitiesForOrganization",
"health:describeEntityAggregates",
"health:describeEntityAggregatesForOrganization",
```



```
"health:describeEventAggregates",
"health:describeEventDetails",
"health:describeEventDetailsForOrganization",
"health:describeEvents",
"health:describeEventsForOrganization",
"health:describeEventTypes",
"health:describeHealthServiceStatusForOrganization",
"iam:getAccessKeyLastUsed",
"iam:getAccountAuthorizationDetails",
"iam:getAccountPasswordPolicy",
"iam:getAccountSummary",
"iam:getContextKeysForCustomPolicy",
"iam:getContextKeysForPrincipalPolicy",
"iam:getCredentialReport",
"iam:getGroup",
"iam:getGroupPolicy",
"iam:getInstanceProfile",
"iam:getLoginProfile",
"iam:getOpenIDConnectProvider",
"iam:getPolicy",
"iam:getPolicyVersion",
"iam:getRole",
"iam:getRolePolicy",
"iam:getSAMLProvider",
"iam:getServerCertificate",
"iam:getServiceLinkedRoleDeletionStatus",
"iam:getSSHPublicKey",
"iam:getUser",
"iam:getUserPolicy",
"iam:listAccessKeys",
"iam:listAccountAliases",
"iam:listAttachedGroupPolicies",
"iam:listAttachedRolePolicies",
"iam:listAttachedUserPolicies",
"iam:listEntitiesForPolicy",
"iam:listGroupPolicies",
"iam:listGroups",
"iam:listGroupsForUser",
"iam:listInstanceProfiles",
"iam:listInstanceProfilesForRole",
"iam:listMFADevices",
"iam:listOpenIDConnectProviders",
"iam:listPolicies",
"iam:listPolicyVersions",
```

```
"iam:listRolePolicies",
"iam:listRoles",
"iam:listSAMLProviders",
"iam:listServerCertificates",
"iam:listSigningCertificates",
"iam:listSSHPublicKeys",
"iam:listUserPolicies",
"iam:listUsers",
"iam:listVirtualMFADevices",
"iam:simulateCustomPolicy",
"iam:simulatePrincipalPolicy",
"imagebuilder:getComponent",
"imagebuilder:getComponentPolicy",
"imagebuilder:getContainerRecipe",
"imagebuilder:getDistributionConfiguration",
"imagebuilder:getImage",
"imagebuilder:getImagePipeline",
"imagebuilder:getImagePolicy",
"imagebuilder:getImageRecipe",
"imagebuilder:getImageRecipePolicy",
"imagebuilder:getInfrastructureConfiguration",
"imagebuilder:getLifecycleExecution",
"imagebuilder:getLifecyclePolicy",
"imagebuilder:getWorkflow",
"imagebuilder:getWorkflowExecution",
"imagebuilder:getWorkflowStepExecution",
"imagebuilder:listComponentBuildVersions",
"imagebuilder:listComponents",
"imagebuilder:listContainerRecipes",
"imagebuilder:listDistributionConfigurations",
"imagebuilder:listImageBuildVersions",
"imagebuilder:listImagePipelineImages",
"imagebuilder:listImagePipelines",
"imagebuilder:listImageRecipes",
"imagebuilder:listImages",
"imagebuilder:listImageScanFindingAggregations",
"imagebuilder:listInfrastructureConfigurations",
"imagebuilder:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowBuildVersions",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflows",
"imagebuilder:listWorkflowStepExecutions",
```

```
"imagebuilder:listTagsForResource",
"inspector:describeAssessmentRuns",
"inspector:describeAssessmentTargets",
"inspector:describeAssessmentTemplates",
"inspector:describeCrossAccountAccessRole",
"inspector:describeResourceGroups",
"inspector:describeRulesPackages",
"inspector:getTelemetryMetadata",
"inspector:listAssessmentRunAgents",
"inspector:listAssessmentRuns",
"inspector:listAssessmentTargets",
"inspector:listAssessmentTemplates",
"inspector:listEventSubscriptions",
"inspector:listRulesPackages",
"inspector:listTagsForResource",
"inspector2:batchGetAccountStatus",
"inspector2:batchGetFreeTrialInfo",
"inspector2:describeOrganizationConfiguration",
"inspector2:getDelegatedAdminAccount",
"inspector2:getMember",
"inspector2:getSbomExport",
"inspector2:listCisScanConfigurations",
"inspector2:listCisScanResultsAggregatedByChecks",
"inspector2:listCisScanResultsAggregatedByTargetResource",
"inspector2:listCisScans",
"inspector2:listCoverage",
"inspector2:listDelegatedAdminAccounts",
"inspector2:listFilters",
"inspector2:listFindings",
"inspector2:listMembers",
"inspector2:listUsageTotals",
"inspector-scan:scanSbom",
"internetmonitor:getMonitor",
"internetmonitor:listMonitors",
"internetmonitor:getHealthEvent",
"internetmonitor:listHealthEvents",
"iot:describeAuthorizer",
"iot:describeCACertificate",
"iot:describeCertificate",
"iot:describeDefaultAuthorizer",
"iot:describeDomainConfiguration",
"iot:describeEndpoint",
"iot:describeIndex",
"iot:describeJobExecution",
```

```
"iot:describeThing",
"iot:describeThingGroup",
"iot:describeTunnel",
"iot:getEffectivePolicies",
"iot:getIndexingConfiguration",
"iot:getLoggingOptions",
"iot:getPolicy",
"iot:getPolicyVersion",
"iot:getTopicRule",
"iot:getV2LoggingOptions",
"iot:listAttachedPolicies",
"iot:listAuthorizers",
"iot:listCACertificates",
"iot:listCertificates",
"iot:listCertificatesByCA",
"iot:listDomainConfigurations",
"iot:listJobExecutionsForJob",
"iot:listJobExecutionsForThing",
"iot:listJobs",
"iot:listNamedShadowsForThing",
"iot:listOutgoingCertificates",
"iot:listPackages",
"iot:listPackageVersions",
"iot:listPolicies",
"iot:listPolicyPrincipals",
"iot:listPolicyVersions",
"iot:listPrincipalPolicies",
"iot:listPrincipalThings",
"iot:listRoleAliases",
"iot:listTargetsForPolicy",
"iot:listThingGroups",
"iot:listThingGroupsForThing",
"iot:listThingPrincipals",
"iot:listThingRegistrationTasks",
"iot:listThings",
"iot:listThingsInThingGroup",
"iot:listThingTypes",
"iot:listTopicRules",
"iot:listTunnels",
"iot:listV2LoggingLevels",
"iotevents:describeDetector",
"iotevents:describeDetectorModel",
"iotevents:describeInput",
"iotevents:describeLoggingOptions",
```

```
"iotevents:listDetectorModels",
"iotevents:listDetectorModelVersions",
"iotevents:listDetectors",
"iotevents:listInputs",
"iotfleetwise:getCampaign",
"iotfleetwise:getDecoderManifest",
"iotfleetwise:getFleet",
"iotfleetwise:getModelManifest",
"iotfleetwise:getSignalCatalog",
"iotfleetwise:getVehicle",
"iotfleetwise:getVehicleStatus",
"iotfleetwise:listCampaigns",
"iotfleetwise:listDecoderManifests",
"iotfleetwise:listDecoderManifestNetworkInterfaces",
"iotfleetwise:listDecoderManifestSignals",
"iotfleetwise:listFleets",
"iotfleetwise:listFleetsForVehicle",
"iotfleetwise:listModelManifests",
"iotfleetwise:listModelManifestNodes",
"iotfleetwise:listSignalCatalogs",
"iotfleetwise:listSignalCatalogNodes",
"iotfleetwise:listVehicles",
"iotsitewise:describeAccessPolicy",
"iotsitewise:describeAsset",
"iotsitewise:describeAssetModel",
"iotsitewise:describeAssetProperty",
"iotsitewise:describeDashboard",
"iotsitewise:describeGateway",
"iotsitewise:describeGatewayCapabilityConfiguration",
"iotsitewise:describeLoggingOptions",
"iotsitewise:describePortal",
"iotsitewise:describeProject",
"iotsitewise:listAccessPolicies",
"iotsitewise:listAssetModels",
"iotsitewise:listAssets",
"iotsitewise:listAssociatedAssets",
"iotsitewise:listDashboards",
"iotsitewise:listGateways",
"iotsitewise:listPortals",
"iotsitewise:listProjectAssets",
"iotsitewise:listProjects",
"iottwinmaker:getComponentType",
"iottwinmaker:getEntity",
"iottwinmaker:getPricingPlan",
```

```
"iottwinmaker:getScene",
"iottwinmaker:getWorkspace",
"iottwinmaker:listComponentTypes",
"iottwinmaker:listEntities",
"iottwinmaker:listScenes",
"iottwinmaker:getSyncJob",
"iottwinmaker:listSyncJobs",
"iottwinmaker:listSyncResources",
"iottwinmaker:listWorkspaces",
"iotwireless:getDestination",
"iotwireless:getDeviceProfile",
"iotwireless:getPartnerAccount",
"iotwireless:getServiceEndpoint",
"iotwireless:getServiceProfile",
"iotwireless:getWirelessDevice",
"iotwireless:getWirelessDeviceStatistics",
"iotwireless:getWirelessGateway",
"iotwireless:getWirelessGatewayCertificate",
"iotwireless:getWirelessGatewayFirmwareInformation",
"iotwireless:getWirelessGatewayStatistics",
"iotwireless:getWirelessGatewayTask",
"iotwireless:getWirelessGatewayTaskDefinition",
"iotwireless:listDestinations",
"iotwireless:listDeviceProfiles",
"iotwireless:listPartnerAccounts",
"iotwireless:listServiceProfiles",
"iotwireless:listTagsForResource",
"iotwireless:listWirelessDevices",
"iotwireless:listWirelessGateways",
"iotwireless:listWirelessGatewayTaskDefinitions",
"ivs:getChannel",
"ivs:getRecordingConfiguration",
"ivs:getStream",
"ivs:getStreamSession",
"ivs:listChannels",
"ivs:listPlaybackKeyPairs",
"ivs:listRecordingConfigurations",
"ivs:listStreamKeys",
"ivs:listStreams",
"ivs:listStreamSessions",
"kafka:describeCluster",
"kafka:describeClusterOperation",
"kafka:describeClusterOperationV2",
"kafka:describeClusterV2",
```

```
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:describeReplicator",
"kafka:describeVpcConnection",
"kafka:getBootstrapBrokers",
"kafka:getClusterPolicy",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClientVpcConnections",
"kafka:listClusterOperations",
"kafka:listClusterOperationsV2",
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"kafka:listReplicators",
"kafka:listScramSecrets",
"kafka:listVpcConnections",
"kafkaconnect:describeConnector",
"kafkaconnect:describeCustomPlugin",
"kafkaconnect:describeWorkerConfiguration",
"kafkaconnect:listConnectors",
"kafkaconnect:listCustomPlugins",
"kafkaconnect:listWorkerConfigurations",
"kendra:describeDataSource",
"kendra:describeFaq",
"kendra:describeIndex",
"kendra:listDataSources",
"kendra:listFaqs",
"kendra:listIndices",
"kinesis:describeStream",
"kinesis:describeStreamConsumer",
"kinesis:describeStreamSummary",
"kinesis:listShards",
"kinesis:listStreams",
"kinesis:listStreamConsumers",
"kinesis:listTagsForStream",
"kinesisanalytics:describeApplication",
"kinesisanalytics:describeApplicationSnapshot",
"kinesisanalytics:listApplications",
"kinesisanalytics:listApplicationSnapshots",
"kinesisvideo:describeImageGenerationConfiguration",
"kinesisvideo:describeNotificationConfiguration",
"kinesisvideo:describeSignalingChannel",
"kinesisvideo:describeStream",
```

```
"kinesisvideo:getDataEndpoint",
"kinesisvideo:getIceServerConfig",
"kinesisvideo:getSignalingChannelEndpoint",
"kinesisvideo:listSignalingChannels",
"kinesisvideo:listStreams",
"kms:describeKey",
"kms:getKeyPolicy",
"kms:getKeyRotationStatus",
"kms:listAliases",
"kms:listGrants",
"kms:listKeyPolicies",
"kms:listKeys",
"kms:listResourceTags",
"kms:listRetirableGrants",
"lambda:getAccountSettings",
"lambda:getAlias",
"lambda:getCodeSigningConfig",
"lambda:getEventSourceMapping",
"lambda:getFunction",
"lambda:getFunctionCodeSigningConfig",
"lambda:getFunctionConcurrency",
"lambda:getFunctionConfiguration",
"lambda:getFunctionEventInvokeConfig",
"lambda:getFunctionUrlConfig",
"lambda:getLayerVersion",
"lambda:getLayerVersionPolicy",
"lambda:getPolicy",
"lambda:getProvisionedConcurrencyConfig",
"lambda:getRuntimeManagementConfig",
"lambda:listAliases",
"lambda:listCodeSigningConfigs",
"lambda:listEventSourceMappings",
"lambda:listFunctionEventInvokeConfigs",
"lambda:listFunctions",
"lambda:listFunctionsByCodeSigningConfig",
"lambda:listFunctionUrlConfigs",
"lambda:listLayers",
"lambda:listLayerVersions",
"lambda:listProvisionedConcurrencyConfigs",
"lambda:listVersionsByFunction",
"launchwizard:describeProvisionedApp",
"launchwizard:describeProvisioningEvents",
"launchwizard:listProvisionedApps",
"lex:describeBot",
```



```
"lex:describeBotAlias",
"lex:describeBotLocale",
"lex:describeBotRecommendation",
"lex:describeBotVersion",
"lex:describeCustomVocabularyMetadata",
"lex:describeExport",
"lex:describeImport",
"lex:describeIntent",
"lex:describeResourcePolicy",
"lex:describeSlot",
"lex:describeSlotType",
"lex:getBot",
"lex:getBotAlias",
"lex:getBotAliases",
"lex:getBotChannelAssociation",
"lex:getBotChannelAssociations",
"lex:getBots",
"lex:getBotVersions",
"lex:getBuiltinIntent",
"lex:getBuiltinIntents",
"lex:getBuiltinSlotTypes",
"lex:getIntent",
"lex:getIntents",
"lex:getIntentVersions",
"lex:getSlotType",
"lex:getSlotTypes",
"lex:getSlotTypeVersions",
"lex:listBotAliases",
"lex:listBotLocales",
"lex:listBotRecommendations",
"lex:listBots",
"lex:listBotVersions",
"lex:listExports",
"lex:listImports",
"lex:listIntents",
"lex:listRecommendedIntents",
"lex:listSlots",
"lex:listSlotTypes",
"license-manager:getLicenseConfiguration",
"license-manager:getServiceSettings",
"license-manager:listAssociationsForLicenseConfiguration",
"license-manager:listFailuresForLicenseConfigurationOperations",
"license-manager:listLicenseConfigurations",
"license-manager:listLicenseSpecificationsForResource",
```

```
"license-manager:listResourceInventory",
"license-manager:listUsageForLicenseConfiguration",
"lightsail:getActiveNames",
"lightsail:getAlarms",
"lightsail:getAutoSnapshots",
"lightsail:getBlueprints",
"lightsail:getBucketBundles",
"lightsail:getBucketMetricData",
"lightsail:getBuckets",
"lightsail:getBundles",
"lightsail:getCertificates",
"lightsail:getContainerImages",
"lightsail:getContainerServiceDeployments",
"lightsail:getContainerServiceMetricData",
"lightsail:getContainerServicePowers",
"lightsail:getContainerServices",
"lightsail:getDisk",
"lightsail:getDisks",
"lightsail:getDiskSnapshot",
"lightsail:getDiskSnapshots",
"lightsail:getDistributionBundles",
"lightsail:getDistributionMetricData",
"lightsail:getDistributions",
"lightsail:getDomain",
"lightsail:getDomains",
"lightsail:getExportSnapshotRecords",
"lightsail:getInstance",
"lightsail:getInstanceMetricData",
"lightsail:getInstancePortStates",
"lightsail:getInstances",
"lightsail:getInstanceSnapshot",
"lightsail:getInstanceSnapshots",
"lightsail:getInstanceState",
"lightsail:getKeyPair",
"lightsail:getKeyPairs",
"lightsail:getLoadBalancer",
"lightsail:getLoadBalancerMetricData",
"lightsail:getLoadBalancers",
"lightsail:getLoadBalancerTlsCertificates",
"lightsail:getOperation",
"lightsail:getOperations",
"lightsail:getOperationsForResource",
"lightsail:getRegions",
"lightsail:getRelationalDatabase",
```

```
"lightsail:getRelationalDatabaseMetricData",
"lightsail:getRelationalDatabases",
"lightsail:getRelationalDatabaseSnapshot",
"lightsail:getRelationalDatabaseSnapshots",
"lightsail:getStaticIp",
"lightsail:getStaticIps",
"lightsail:isVpcPeered",
"logs:describeAccountPolicies",
"logs:describeDeliveries",
"logs:describeDeliveryDestinations",
"logs:describeDeliverySources",
"logs:describeDestinations",
"logs:describeExportTasks",
"logs:describeLogGroups",
"logs:describeLogStreams",
"logs:describeMetricFilters",
"logs:describeQueries",
"logs:describeQueryDefinitions",
"logs:describeResourcePolicies",
"logs:describeSubscriptionFilters",
"logs:getDataProtectionPolicy",
"logs:getDelivery",
"logs:getDeliveryDestination",
"logs:getDeliveryDestinationPolicy",
"logs:getDeliverySource",
"logs:getLogAnomalyDetector",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listAnomalies",
"logs:listLogAnomalyDetectors",
"logs:listLogDeliveries",
"logs:testMetricFilter",
"lookoutequipment:describeDataIngestionJob",
"lookoutequipment:describeDataset",
"lookoutequipment:describeInferenceScheduler",
"lookoutequipment:describeModel",
"lookoutequipment:listDataIngestionJobs",
"lookoutequipment:listDatasets",
"lookoutequipment:listInferenceExecutions",
"lookoutequipment:listInferenceSchedulers",
"lookoutequipment:listModels",
"lookoutmetrics:describeAlert",
"lookoutmetrics:describeAnomalyDetectionExecutions",
"lookoutmetrics:describeAnomalyDetector",
```

```
"lookoutmetrics:describeMetricSet",
"lookoutmetrics:getAnomalyGroup",
"lookoutmetrics:getDataQualityMetrics",
"lookoutmetrics:getFeedback",
"lookoutmetrics:getSampleData",
"lookoutmetrics:listAlerts",
"lookoutmetrics:listAnomalyDetectors",
"lookoutmetrics:listAnomalyGroupSummaries",
"lookoutmetrics:listAnomalyGroupTimeSeries",
"lookoutmetrics:listMetricSets",
"lookoutmetrics:listTagsForResource",
"machinelearning:describeBatchPredictions",
"machinelearning:describeDataSources",
"machinelearning:describeEvaluations",
"machinelearning:describeMLModels",
"machinelearning:getBatchPrediction",
"machinelearning:getDataSource",
"machinelearning:getEvaluation",
"machinelearning:getMLModel",
"macie2:getClassificationExportConfiguration",
"macie2:getCustomDataIdentifier",
"macie2:getFindings",
"macie2:getFindingStatistics",
"macie2:listClassificationJobs",
"macie2:listCustomDataIdentifiers",
"macie2:listFindings",
"managedblockchain:getMember",
"managedblockchain:getNetwork",
"managedblockchain:getNode",
"managedblockchain:listMembers",
"managedblockchain:listNetworks",
"managedblockchain:listNodes",
"mediaconnect:describeFlow",
"mediaconnect:listEntitlements",
"mediaconnect:listFlows",
"mediaconvert:describeEndpoints",
"mediaconvert:getJob",
"mediaconvert:getJobTemplate",
"mediaconvert:getPreset",
"mediaconvert:getQueue",
"mediaconvert:listJobs",
"mediaconvert:listJobTemplates",
"medialive:describeChannel",
"medialive:describeInput",
```

```
"medialive:describeInputDevice",
"medialive:describeInputSecurityGroup",
"medialive:describeMultiplex",
"medialive:describeOffering",
"medialive:describeReservation",
"medialive:describeSchedule",
"medialive:listChannels",
"medialive:listInputDevices",
"medialive:listInputs",
"medialive:listInputSecurityGroups",
"medialive:listMultiplexes",
"medialive:listOfferings",
"medialive:listReservations",
"mediapackage:describeChannel",
"mediapackage:describeOriginEndpoint",
"mediapackage:listChannels",
"mediapackage:listOriginEndpoints",
"mediastore:describeContainer",
"mediastore:getContainerPolicy",
"mediastore:getCorsPolicy",
"mediastore:listContainers",
"mediatailor:getPlaybackConfiguration",
"mediatailor:listPlaybackConfigurations",
"medical-imaging:getDatastore",
"medical-imaging:listDatastores",
"mgn:describeJobLogItems",
"mgn:describeJobs",
"mgn:describeLaunchConfigurationTemplates",
"mgn:describeReplicationConfigurationTemplates",
"mgn:describeSourceServers",
"mgn:describeVcenterClients",
"mgn:getLaunchConfiguration",
"mgn:getReplicationConfiguration",
"mgn:listApplications",
"mgn:listSourceServerActions",
"mgn:listTemplateActions",
"mgn:listWaves",
"mobiletargeting:getAdmChannel",
"mobiletargeting:getApnsChannel",
"mobiletargeting:getApnsSandboxChannel",
"mobiletargeting:getApnsVoipChannel",
"mobiletargeting:getApnsVoipSandboxChannel",
"mobiletargeting:getApp",
"mobiletargeting:getApplicationSettings",
```

```
"mobiletargeting:getApps",
"mobiletargeting:getBaiduChannel",
"mobiletargeting:getCampaign",
"mobiletargeting:getCampaignActivities",
"mobiletargeting:getCampaigns",
"mobiletargeting:getCampaignVersion",
"mobiletargeting:getCampaignVersions",
"mobiletargeting:getEmailChannel",
"mobiletargeting:getEndpoint",
"mobiletargeting:getEventStream",
"mobiletargeting:getExportJob",
"mobiletargeting:getExportJobs",
"mobiletargeting:getGcmChannel",
"mobiletargeting:getImportJob",
"mobiletargeting:getImportJobs",
"mobiletargeting:getJourney",
"mobiletargeting:getJourneyExecutionMetrics",
"mobiletargeting:getJourneyExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionMetrics",
"mobiletargeting:getJourneyRuns",
"mobiletargeting:getSegment",
"mobiletargeting:getSegmentImportJobs",
"mobiletargeting:getSegments",
"mobiletargeting:getSegmentVersion",
"mobiletargeting:getSegmentVersions",
"mobiletargeting:getSmsChannel",
"mobiletargeting:listJourneys",
"mq:describeBroker",
"mq:describeConfiguration",
"mq:describeConfigurationRevision",
"mq:describeUser",
"mq:listBrokers",
"mq:listConfigurationRevisions",
"mq:listConfigurations",
"mq:listUsers",
"m2:getApplication",
"m2:getApplicationVersion",
"m2:getBatchJobExecution",
"m2:getDataSetDetails",
"m2:getDataSetImportTask",
"m2:getDeployment",
"m2:getEnvironment",
"m2:listApplications",
```

```
"m2:listApplicationVersions",
"m2:listBatchJobDefinitions",
"m2:listBatchJobExecutions",
"m2:listDataSetImportHistory",
"m2:listDataSets",
"m2:listDeployments",
"m2:listEngineVersions",
"m2:listEnvironments",
"network-firewall:describeFirewall",
"network-firewall:describeFirewallPolicy",
"network-firewall:describeLoggingConfiguration",
"network-firewall:describeRuleGroup",
"network-firewall:describeTlsInspectionConfiguration",
"network-firewall:listFirewallPolicies",
"network-firewall:listFirewalls",
"network-firewall:listRuleGroups",
"network-firewall:listTlsInspectionConfigurations",
"networkmanager:describeGlobalNetworks",
"networkmanager:getConnectAttachment",
"networkmanager:getConnections",
"networkmanager:getConnectPeer",
"networkmanager:getConnectPeerAssociations",
"networkmanager:getCoreNetwork",
"networkmanager:getCoreNetworkChangeEvents",
"networkmanager:getCoreNetworkChangeSet",
"networkmanager:getCoreNetworkPolicy",
"networkmanager:getCustomerGatewayAssociations",
"networkmanager:getDevices",
"networkmanager:getLinkAssociations",
"networkmanager:getLinks",
"networkmanager:getNetworkResourceCounts",
"networkmanager:getNetworkResourceRelationships",
"networkmanager:getNetworkResources",
"networkmanager:getNetworkRoutes",
"networkmanager:getNetworkTelemetry",
"networkmanager:getResourcePolicy",
"networkmanager:getRouteAnalysis",
"networkmanager:getSites",
"networkmanager:getSiteToSiteVpnAttachment",
"networkmanager:getTransitGatewayConnectPeerAssociations",
"networkmanager:getTransitGatewayPeering",
"networkmanager:getTransitGatewayRegistrations",
"networkmanager:getTransitGatewayRouteTableAttachment",
"networkmanager:getVpcAttachment",
```

```
"networkmanager:listAttachments",
"networkmanager:listConnectPeers",
"networkmanager:listCoreNetworkPolicyVersions",
"networkmanager:listCoreNetworks",
"networkmanager:listOrganizationServiceAccessStatus",
"networkmanager:listPeerings",
"networkmanager:listTagsForResource",
"networkmonitor:getMonitor",
"networkmonitor:getProbe",
"networkmonitor:listMonitors",
"nimble:getEula",
"nimble:getLaunchProfile",
"nimble:getLaunchProfileDetails",
"nimble:getLaunchProfileInitialization",
"nimble:getLaunchProfileMember",
"nimble:getStreamingImage",
"nimble:getStreamingSession",
"nimble:getStreamingSessionStream",
"nimble:getStudio",
"nimble:getStudioComponent",
"nimble:listEulaAcceptances",
"nimble:listEulas",
"nimble:listLaunchProfiles",
"nimble:listStreamingImages",
"nimble:listStreamingSessions",
"nimble:listStudioComponents",
"nimble:listStudios",
"notifications:getEventRule",
"notifications:getNotificationConfiguration",
"notifications:getNotificationEvent",
"notifications:listChannels",
"notifications:listEventRules",
"notifications:listNotificationConfigurations",
"notifications:listNotificationEvents",
"notifications:listNotificationHubs",
"notifications-contacts:getEmailContact",
"notifications-contacts:listEmailContacts",
"oam:getLink",
"oam:getSink",
"oam:getSinkPolicy",
"oam:listAttachedLinks",
"oam:listLinks",
"oam:listSinks",
"omics:getAnnotationImportJob",
```



```
"omics:getAnnotationStore",
"omics:getReadSetImportJob",
"omics:getReadSetMetadata",
"omics:getReference",
"omics:getReferenceImportJob",
"omics:getReferenceMetadata",
"omics:getReferenceStore",
"omics:getRun",
"omics:getRunGroup",
"omics:getSequenceStore",
"omics:getVariantImportJob",
"omics:getVariantStore",
"omics:getWorkflow",
"omics:listAnnotationImportJobs",
"omics:listAnnotationStores",
"omics:listMultipartReadSetUploads",
"omics:listReadSetImportJobs",
"omics:listReadSets",
"omics:listReadSetUploadParts",
"omics:listReferenceImportJobs",
"omics:listReferenceStores",
"omics:listReferences",
"omics:listRunGroups",
"omics:listRunTasks",
"omics:listRuns",
"omics:listSequenceStores",
"omics:listVariantImportJobs",
"omics:listVariantStores",
"omics:listWorkflows",
"opsworks-cm:describeAccountAttributes",
"opsworks-cm:describeBackups",
"opsworks-cm:describeEvents",
"opsworks-cm:describeNodeAssociationStatus",
"opsworks-cm:describeServers",
"opsworks:describeAgentVersions",
"opsworks:describeApps",
"opsworks:describeCommands",
"opsworks:describeDeployments",
"opsworks:describeEcsClusters",
"opsworks:describeElasticIps",
"opsworks:describeElasticLoadBalancers",
"opsworks:describeInstances",
"opsworks:describeLayers",
"opsworks:describeLoadBasedAutoScaling",
```

```
"opsworks:describeMyUserProfile",
"opsworks:describePermissions",
"opsworks:describeRaidArrays",
"opsworks:describeRdsDbInstances",
"opsworks:describeServiceErrors",
"opsworks:describeStackProvisioningParameters",
"opsworks:describeStacks",
"opsworks:describeStackSummary",
"opsworks:describeTimeBasedAutoScaling",
"opsworks:describeUserProfiles",
"opsworks:describeVolumes",
"opsworks:getHostnameSuggestion",
"organizations:listAccounts",
"organizations:listTagsForResource",
"outposts:getCatalogItem",
"outposts:getConnection",
"outposts:getOrder",
"outposts:getOutpost",
"outposts:getOutpostInstanceTypes",
"outposts:getSite",
"outposts:listAssets",
"outposts:listCatalogItems",
"outposts:listOrders",
"outposts:listOutposts",
"outposts:listSites",
"personalize:describeAlgorithm",
"personalize:describeBatchInferenceJob",
"personalize:describeBatchSegmentJob",
"personalize:describeCampaign",
"personalize:describeDataset",
"personalize:describeDatasetExportJob",
"personalize:describeDatasetGroup",
"personalize:describeDatasetImportJob",
"personalize:describeEventTracker",
"personalize:describeFeatureTransformation",
"personalize:describeFilter",
"personalize:describeRecipe",
"personalize:describeRecommender",
"personalize:describeSchema",
"personalize:describeSolution",
"personalize:describeSolutionVersion",
"personalize:getPersonalizedRanking",
"personalize:getRecommendations",
"personalize:getSolutionMetrics",
```

```
"personalize:listBatchInferenceJobs",
"personalize:listBatchSegmentJobs",
"personalize:listCampaigns",
"personalize:listDatasetExportJobs",
"personalize:listDatasetGroups",
"personalize:listDatasetImportJobs",
"personalize:listDatasets",
"personalize:listEventTrackers",
"personalize:listRecipes",
"personalize:listRecommenders",
"personalize:listSchemas",
"personalize:listSolutions",
"personalize:listSolutionVersions",
"pipes:describePipe",
"pipes:listPipes",
"pipes:listTagsForResource",
"polly:describeVoices",
"polly:getLexicon",
"polly:listLexicons",
"pricing:describeServices",
"pricing:getAttributeValues",
"pricing:getProducts",
"private-networks:getDeviceIdentifier",
"private-networks:getNetwork",
"private-networks:getNetworkResource",
"private-networks:listDeviceIdentifiers",
"private-networks:listNetworks",
"private-networks:listNetworkResources",
"qbusiness:getApplication",
"qbusiness:getDataSource",
"qbusiness:getIndex",
"qbusiness:getRetriever",
"qbusiness:getWebExperience",
"qbusiness:listApplications",
"qbusiness:listDataSources",
"qbusiness:listDataSourceSyncJobs",
"qbusiness:listIndices",
"qbusiness:listRetrievers",
"qbusiness:listWebExperiences",
"quicksight:describeAccountCustomization",
"quicksight:describeAccountSettings",
"quicksight:describeAccountSubscription",
"quicksight:describeAnalysis",
"quicksight:describeAnalysisPermissions",
```

```
"quicksight:describeDashboard",
"quicksight:describeDashboardPermissions",
"quicksight:describeDataSet",
"quicksight:describeDataSetPermissions",
"quicksight:describeDataSetRefreshProperties",
"quicksight:describeDataSource",
"quicksight:describeDataSourcePermissions",
"quicksight:describeFolder",
"quicksight:describeFolderPermissions",
"quicksight:describeFolderResolvedPermissions",
"quicksight:describeGroup",
"quicksight:describeGroupMembership",
"quicksight:describeIAMPolicyAssignment",
"quicksight:describeIngestion",
"quicksight:describeIpRestriction",
"quicksight:describeNamespace",
"quicksight:describeRefreshSchedule",
"quicksight:describeTemplate",
"quicksight:describeTemplateAlias",
"quicksight:describeTemplatePermissions",
"quicksight:describeTheme",
"quicksight:describeThemeAlias",
"quicksight:describeThemePermissions",
"quicksight:describeTopic",
"quicksight:describeTopicPermissions",
"quicksight:describeTopicRefresh",
"quicksight:describeTopicRefreshSchedule",
"quicksight:describeUser",
"quicksight:describeVPCConnection",
"quicksight:listAnalyses",
"quicksight:listDashboards",
"quicksight:listDashboardVersions",
"quicksight:listDataSets",
"quicksight:listDataSources",
"quicksight:listFolderMembers",
"quicksight:listFolders",
"quicksight:listGroupMemberships",
"quicksight:listGroups",
"quicksight:listIAMPolicyAssignments",
"quicksight:listIAMPolicyAssignmentsForUser",
"quicksight:listIngestions",
"quicksight:listNamespaces",
"quicksight:listRefreshSchedules",
"quicksight:listTemplateAliases",
```

```
"quicksight:listTemplates",
"quicksight:listTemplateVersions",
"quicksight:listThemeAliases",
"quicksight:listThemes",
"quicksight:listThemeVersions",
"quicksight:listTopicRefreshSchedules",
"quicksight:listTopics",
"quicksight:listUserGroups",
"quicksight:listUsers",
"quicksight:listVPCConnections",
"quicksight:searchAnalyses",
"quicksight:searchDashboards",
"quicksight:searchDataSets",
"quicksight:searchDataSources",
"quicksight:searchFolders",
"quicksight:searchGroups",
"ram:getPermission",
"ram:getResourceShareAssociations",
"ram:getResourceShareInvitations",
"ram:getResourceShares",
"ram:listPendingInvitationResources",
"ram:listPrincipals",
"ram:listResources",
"ram:listResourceSharePermissions",
"rbin:getRule",
"rbin:listRules",
"rds:describeAccountAttributes",
"rds:describeBlueGreenDeployments",
"rds:describeCertificates",
"rds:describeDBClusterEndpoints",
"rds:describeDBClusterParameterGroups",
"rds:describeDBClusterParameters",
"rds:describeDBClusters",
"rds:describeDBClusterSnapshots",
"rds:describeDBEngineVersions",
"rds:describeDBInstanceAutomatedBackups",
"rds:describeDBInstances",
"rds:describeDBLogFiles",
"rds:describeDBParameterGroups",
"rds:describeDBParameters",
"rds:describeDBSecurityGroups",
"rds:describeDBSnapshotAttributes",
"rds:describeDBSnapshots",
"rds:describeDBSubnetGroups",
```

```
"rds:describeEngineDefaultClusterParameters",
"rds:describeEngineDefaultParameters",
"rds:describeEventCategories",
"rds:describeEvents",
"rds:describeEventSubscriptions",
"rds:describeExportTasks",
"rds:describeGlobalClusters",
"rds:describeIntegrations",
"rds:describeOptionGroupOptions",
"rds:describeOptionGroups",
"rds:describeOrderableDBInstanceOptions",
"rds:describePendingMaintenanceActions",
"rds:describeReservedDBInstances",
"rds:describeReservedDBInstancesOfferings",
"rds:describeSourceRegions",
"rds:describeValidDBInstanceModifications",
"rds:listTagsForResource",
"redshift-data:describeStatement",
"redshift-data:listStatements",
"redshift:describeClusterParameterGroups",
"redshift:describeClusterParameters",
"redshift:describeClusters",
"redshift:describeClusterSecurityGroups",
"redshift:describeClusterSnapshots",
"redshift:describeClusterSubnetGroups",
"redshift:describeClusterVersions",
"redshift:describeDataShares",
"redshift:describeDataSharesForConsumer",
"redshift:describeDataSharesForProducer",
"redshift:describeDefaultClusterParameters",
"redshift:describeEventCategories",
"redshift:describeEvents",
"redshift:describeEventSubscriptions",
"redshift:describeHsmClientCertificates",
"redshift:describeHsmConfigurations",
"redshift:describeLoggingStatus",
"redshift:describeOrderableClusterOptions",
"redshift:describeReservedNodeOfferings",
"redshift:describeReservedNodes",
"redshift:describeResize",
"redshift:describeSnapshotCopyGrants",
"redshift:describeStorage",
"redshift:describeTableRestoreStatus",
"redshift:describeTags",
```

```
"redshift-serverless:getEndpointAccess",
"redshift-serverless:getNamespace",
"redshift-serverless:getRecoveryPoint",
"redshift-serverless:getSnapshot",
"redshift-serverless:getTableRestoreStatus",
"redshift-serverless:getUsageLimit",
"redshift-serverless:getWorkgroup",
"redshift-serverless:listEndpointAccess",
"redshift-serverless:listNamespaces",
"redshift-serverless:listRecoveryPoints",
"redshift-serverless:listSnapshots",
"redshift-serverless:listTableRestoreStatus",
"redshift-serverless:listUsageLimits",
"redshift-serverless:listWorkgroups",
"rekognition:listCollections",
"rekognition:listFaces",
"resource-explorer-2:getAccountLevelServiceConfiguration",
"resource-explorer-2:getIndex",
"resource-explorer-2:getView",
"resource-explorer-2:listIndexes",
"resource-explorer-2:listViews",
"resource-explorer-2:search",
"resource-groups:getGroup",
"resource-groups:getGroupQuery",
"resource-groups:getTags",
"resource-groups:listGroupResources",
"resource-groups:listGroups",
"resource-groups:searchResources",
"robomaker:batchDescribeSimulationJob",
"robomaker:describeDeploymentJob",
"robomaker:describeFleet",
"robomaker:describeRobot",
"robomaker:describeRobotApplication",
"robomaker:describeSimulationApplication",
"robomaker:describeSimulationJob",
"robomaker:listDeploymentJobs",
"robomaker:listFleets",
"robomaker:listRobotApplications",
"robomaker:listRobots",
"robomaker:listSimulationApplications",
"robomaker:listSimulationJobs",
"route53-recovery-cluster:getRoutingControlState",
"route53-recovery-cluster:listRoutingControls",
"route53-recovery-control-config:describeControlPanel",
```

```
"route53-recovery-control-config:describeRoutingControl",
"route53-recovery-control-config:describeSafetyRule",
"route53-recovery-control-config:listControlPanels",
"route53-recovery-control-config:listRoutingControls",
"route53-recovery-control-config:listSafetyRules",
"route53-recovery-readiness:getCell",
"route53-recovery-readiness:getCellReadinessSummary",
"route53-recovery-readiness:getReadinessCheck",
"route53-recovery-readiness:getReadinessCheckResourceStatus",
"route53-recovery-readiness:getReadinessCheckStatus",
"route53-recovery-readiness:getRecoveryGroup",
"route53-recovery-readiness:getRecoveryGroupReadinessSummary",
"route53-recovery-readiness:listCells",
"route53-recovery-readiness:listReadinessChecks",
"route53-recovery-readiness:listRecoveryGroups",
"route53-recovery-readiness:listResourceSets",
"route53:getAccountLimit",
"route53:getChange",
"route53:getCheckerIpRanges",
"route53:getDNSSEC",
"route53:getGeoLocation",
"route53:getHealthCheck",
"route53:getHealthCheckCount",
"route53:getHealthCheckLastFailureReason",
"route53:getHealthCheckStatus",
"route53:getHostedZone",
"route53:getHostedZoneCount",
"route53:getHostedZoneLimit",
"route53:getQueryLoggingConfig",
"route53:getReusableDelegationSet",
"route53:getTrafficPolicy",
"route53:getTrafficPolicyInstance",
"route53:getTrafficPolicyInstanceCount",
"route53:listCidrBlocks",
"route53:listCidrCollections",
"route53:listCidrLocations",
"route53:listGeoLocations",
"route53:listHealthChecks",
"route53:listHostedZones",
"route53:listHostedZonesByName",
"route53:listHostedZonesByVpc",
"route53:listQueryLoggingConfigs",
"route53:listResourceRecordSets",
"route53:listReusableDelegationSets",
```



```
"route53:listTrafficPolicies",
"route53:listTrafficPolicyInstances",
"route53:listTrafficPolicyInstancesByHostedZone",
"route53:listTrafficPolicyInstancesByPolicy",
"route53:listTrafficPolicyVersions",
"route53:listVPCAssociationAuthorizations",
"route53domains:checkDomainAvailability",
"route53domains:getContactReachabilityStatus",
"route53domains:getDomainDetail",
"route53domains:getOperationDetail",
"route53domains:listDomains",
"route53domains:listOperations",
"route53domains:listPrices",
"route53domains:listTagsForDomain",
"route53domains:viewBilling",
"route53resolver:getFirewallConfig",
"route53resolver:getFirewallDomainList",
"route53resolver:getFirewallRuleGroup",
"route53resolver:getFirewallRuleGroupAssociation",
"route53resolver:getFirewallRuleGroupPolicy",
"route53resolver:getOutpostResolver",
"route53resolver:getResolverDnssecConfig",
"route53resolver:getResolverQueryLogConfig",
"route53resolver:getResolverQueryLogConfigAssociation",
"route53resolver:getResolverQueryLogConfigPolicy",
"route53resolver:getResolverRule",
"route53resolver:getResolverRuleAssociation",
"route53resolver:getResolverRulePolicy",
"route53resolver:listFirewallConfigs",
"route53resolver:listFirewallDomainLists",
"route53resolver:listFirewallDomains",
"route53resolver:listFirewallRuleGroupAssociations",
"route53resolver:listFirewallRuleGroups",
"route53resolver:listFirewallRules",
"route53resolver:listOutpostResolvers",
"route53resolver:listResolverConfigs",
"route53resolver:listResolverDnssecConfigs",
"route53resolver:listResolverEndpointIpAddresses",
"route53resolver:listResolverEndpoints",
"route53resolver:listResolverQueryLogConfigAssociations",
"route53resolver:listResolverQueryLogConfigs",
"route53resolver:listResolverRuleAssociations",
"route53resolver:listResolverRules",
"route53resolver:listTagsForResource",
```

```
"rum:batchGetRumMetricDefinitions",
"rum:getAppMonitor",
"rum:listAppMonitors",
"rum:listRumMetricsDestinations",
"s3:describeJob",
"s3:describeMultiRegionAccessPointOperation",
"s3:getAccelerateConfiguration",
"s3:getAccessPoint",
"s3:getAccessPointConfigurationForObjectLambda",
"s3:getAccessPointForObjectLambda",
"s3:getAccessPointPolicy",
"s3:getAccessPointPolicyForObjectLambda",
"s3:getAccessPointPolicyStatus",
"s3:getAccessPointPolicyStatusForObjectLambda",
"s3:getAccountPublicAccessBlock",
"s3:getAnalyticsConfiguration",
"s3:getBucketAcl",
"s3:getBucketCORS",
"s3:getBucketLocation",
"s3:getBucketLogging",
"s3:getBucketNotification",
"s3:getBucketObjectLockConfiguration",
"s3:getBucketOwnershipControls",
"s3:getBucketPolicy",
"s3:getBucketPolicyStatus",
"s3:getBucketPublicAccessBlock",
"s3:getBucketRequestPayment",
"s3:getBucketVersioning",
"s3:getBucketWebsite",
"s3:getEncryptionConfiguration",
"s3:getIntelligentTieringConfiguration",
"s3:getInventoryConfiguration",
"s3:getLifecycleConfiguration",
"s3:getMetricsConfiguration",
"s3:getMultiRegionAccessPoint",
"s3:getMultiRegionAccessPointPolicy",
"s3:getMultiRegionAccessPointPolicyStatus",
"s3:getMultiRegionAccessPointRoutes",
"s3:getObjectLegalHold",
"s3:getObjectRetention",
"s3:getReplicationConfiguration",
"s3:getStorageLensConfiguration",
"s3:listAccessPoints",
"s3:listAccessPointsForObjectLambda",
```

```
"s3:listAllMyBuckets",
"s3:listBucket",
"s3:listBucketMultipartUploads",
"s3:listBucketVersions",
"s3:listJobs",
"s3:listMultipartUploadParts",
"s3:listMultiRegionAccessPoints",
"s3:listStorageLensConfigurations",
"s3express:getBucketPolicy",
"s3express:listAllMyDirectoryBuckets",
"sagemaker:describeAction",
"sagemaker:describeAlgorithm",
"sagemaker:describeApp",
"sagemaker:describeAppImageConfig",
"sagemaker:describeArtifact",
"sagemaker:describeAutoMLJob",
"sagemaker:describeCluster",
"sagemaker:describeClusterNode",
"sagemaker:describeCodeRepository",
"sagemaker:describeCompilationJob",
"sagemaker:describeContext",
"sagemaker:describeDataQualityJobDefinition",
"sagemaker:describeDevice",
"sagemaker:describeDeviceFleet",
"sagemaker:describeDomain",
"sagemaker:describeEdgeDeploymentPlan",
"sagemaker:describeEdgePackagingJob",
"sagemaker:describeEndpoint",
"sagemaker:describeEndpointConfig",
"sagemaker:describeExperiment",
"sagemaker:describeFeatureGroup",
"sagemaker:describeFeatureMetadata",
"sagemaker:describeFlowDefinition",
"sagemaker:describeHub",
"sagemaker:describeHubContent",
"sagemaker:describeHumanTaskUi",
"sagemaker:describeHyperParameterTuningJob",
"sagemaker:describeImage",
"sagemaker:describeImageVersion",
"sagemaker:describeInferenceComponent",
"sagemaker:describeInferenceExperiment",
"sagemaker:describeInferenceRecommendationsJob",
"sagemaker:describeLabelingJob",
"sagemaker:describeModel",
```

```
"sagemaker:describeModelBiasJobDefinition",
"sagemaker:describeModelCard",
"sagemaker:describeModelCardExportJob",
"sagemaker:describeModelExplainabilityJobDefinition",
"sagemaker:describeModelPackage",
"sagemaker:describeModelPackageGroup",
"sagemaker:describeModelQualityJobDefinition",
"sagemaker:describeMonitoringSchedule",
"sagemaker:describeNotebookInstance",
"sagemaker:describeNotebookInstanceLifecycleConfig",
"sagemaker:describePipeline",
"sagemaker:describePipelineDefinitionForExecution",
"sagemaker:describePipelineExecution",
"sagemaker:describeProcessingJob",
"sagemaker:describeProject",
"sagemaker:describeSpace",
"sagemaker:describeStudioLifecycleConfig",
"sagemaker:describeSubscribedWorkteam",
"sagemaker:describeTrainingJob",
"sagemaker:describeTransformJob",
"sagemaker:describeTrial",
"sagemaker:describeTrialComponent",
"sagemaker:describeUserProfile",
"sagemaker:describeWorkforce",
"sagemaker:describeWorkteam",
"sagemaker:getDeviceFleetReport",
"sagemaker:getModelPackageGroupPolicy",
"sagemaker:getSagemakerServicecatalogPortfolioStatus",
"sagemaker:listActions",
"sagemaker:listAlgorithms",
"sagemaker:listAliases",
"sagemaker:listAppImageConfigs",
"sagemaker:listApps",
"sagemaker:listArtifacts",
"sagemaker:listAssociations",
"sagemaker:listAutoMLJobs",
"sagemaker:listCandidatesForAutoMLJob",
"sagemaker:listClusterNodes",
"sagemaker:listClusters",
"sagemaker:listCodeRepositories",
"sagemaker:listCompilationJobs",
"sagemaker:listContexts",
"sagemaker:listDataQualityJobDefinitions",
"sagemaker:listDeviceFleets",
```

```
"sagemaker:listDevices",
"sagemaker:listDomains",
"sagemaker:listEdgeDeploymentPlans",
"sagemaker:listEdgePackagingJobs",
"sagemaker:listEndpointConfigs",
"sagemaker:listEndpoints",
"sagemaker:listExperiments",
"sagemaker:listFeatureGroups",
"sagemaker:listFlowDefinitions",
"sagemaker:listHubContents",
"sagemaker:listHubContentVersions",
"sagemaker:listHubs",
"sagemaker:listHumanTaskUis",
"sagemaker:listHyperParameterTuningJobs",
"sagemaker:listImages",
"sagemaker:listImageVersions",
"sagemaker:listInferenceComponents",
"sagemaker:listInferenceExperiments",
"sagemaker:listInferenceRecommendationsJobs",
"sagemaker:listInferenceRecommendationsJobSteps",
"sagemaker:listLabelingJobs",
"sagemaker:listLabelingJobsForWorkteam",
"sagemaker:listLineageGroups",
"sagemaker:listModelBiasJobDefinitions",
"sagemaker:listModelCardExportJobs",
"sagemaker:listModelCards",
"sagemaker:listModelCardVersions",
"sagemaker:listModelExplainabilityJobDefinitions",
"sagemaker:listModelMetadata",
"sagemaker:listModelPackageGroups",
"sagemaker:listModelPackages",
"sagemaker:listModelQualityJobDefinitions",
"sagemaker:listModels",
"sagemaker:listMonitoringAlertHistory",
"sagemaker:listMonitoringAlerts",
"sagemaker:listMonitoringExecutions",
"sagemaker:listMonitoringSchedules",
"sagemaker:listNotebookInstanceLifecycleConfigs",
"sagemaker:listNotebookInstances",
"sagemaker:listPipelineExecutions",
"sagemaker:listPipelineExecutionSteps",
"sagemaker:listPipelineParametersForExecution",
"sagemaker:listPipelines",
"sagemaker:listProcessingJobs",
```

```
"sagemaker:listProjects",
"sagemaker:listSpaces",
"sagemaker:listStageDevices",
"sagemaker:listStudioLifecycleConfigs",
"sagemaker:listSubscribedWorkteams",
"sagemaker:listTags",
"sagemaker:listTrainingJobs",
"sagemaker:listTrainingJobsForHyperParameterTuningJob",
"sagemaker:listTransformJobs",
"sagemaker:listTrialComponents",
"sagemaker:listTrials",
"sagemaker:listUserProfiles",
"sagemaker:listWorkforces",
"sagemaker:listWorkteams",
"savingsplans:describeSavingsPlans",
"scheduler:getSchedule",
"scheduler:getScheduleGroup",
"scheduler:listScheduleGroups",
"scheduler:listSchedules",
"schemas:describeCodeBinding",
"schemas:describeDiscoverer",
"schemas:describeRegistry",
"schemas:describeSchema",
"schemas:getCodeBindingSource",
"schemas:getDiscoveredSchema",
"schemas:getResourcePolicy",
"schemas:listDiscoverers",
"schemas:listRegistries",
"schemas:listSchemas",
"schemas:listSchemaVersions",
"sdb:domainMetadata",
"sdb:listDomains",
"secretsmanager:describeSecret",
"secretsmanager:getResourcePolicy",
"secretsmanager:listSecrets",
"secretsmanager:listSecretVersionIds",
"securityhub:getEnabledStandards",
"securityhub:getFindings",
"securityhub:getInsightResults",
"securityhub:getInsights",
"securityhub:getMasterAccount",
"securityhub:getMembers",
"securityhub:listEnabledProductsForImport",
"securityhub:listInvitations",
```

```
"securityhub:listMembers",
"securitylake:getDataLakeExceptionSubscription",
"securitylake:getDataLakeOrganizationConfiguration",
"securitylake:getDataLakeSources",
"securitylake:getSubscriber",
"securitylake:listDataLakeExceptions",
"securitylake:listDataLakes",
"securitylake:listLogSources",
"securitylake:listSubscribers",
"serverlessrepo:getApplication",
"serverlessrepo:getApplicationPolicy",
"serverlessrepo:getCloudFormationTemplate",
"serverlessrepo:listApplicationDependencies",
"serverlessrepo:listApplications",
"serverlessrepo:listApplicationVersions",
"servicecatalog:describeConstraint",
"servicecatalog:describePortfolio",
"servicecatalog:describeProduct",
"servicecatalog:describeProductAsAdmin",
"servicecatalog:describeProductView",
"servicecatalog:describeProvisioningArtifact",
"servicecatalog:describeProvisioningParameters",
"servicecatalog:describeRecord",
"servicecatalog:listAcceptedPortfolioShares",
"servicecatalog:listConstraintsForPortfolio",
"servicecatalog:listLaunchPaths",
"servicecatalog:listPortfolioAccess",
"servicecatalog:listPortfolios",
"servicecatalog:listPortfoliosForProduct",
"servicecatalog:listPrincipalsForPortfolio",
"servicecatalog:listProvisioningArtifacts",
"servicecatalog:listRecordHistory",
"servicecatalog:scanProvisionedProducts",
"servicecatalog:searchProducts",
"servicequotas:getAssociationForServiceQuotaTemplate",
"servicequotas:getAWSDefaultServiceQuota",
"servicequotas:getRequestedServiceQuotaChange",
"servicequotas:getServiceQuota",
"servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:listAWSDefaultServiceQuotas",
"servicequotas:listRequestedServiceQuotaChangeHistory",
"servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:listServiceQuotas",
```

```
"servicequotas:listServices",
"ses:describeActiveReceiptRuleSet",
"ses:describeConfigurationSet",
"ses:describeReceiptRule",
"ses:describeReceiptRuleSet",
"ses:getAccount",
"ses:getAccountSendingEnabled",
"ses:getBlacklistReports",
"ses:getConfigurationSet",
"ses:getConfigurationSetEventDestinations",
"ses:getContactList",
"ses:getDedicatedIp",
"ses:getDedicatedIpPool",
"ses:getDedicatedIps",
"ses:getDeliverabilityDashboardOptions",
"ses:getDeliverabilityTestReport",
"ses:getDomainDeliverabilityCampaign",
"ses:getDomainStatisticsReport",
"ses:getEmailIdentity",
"ses:getIdentityDkimAttributes",
"ses:getIdentityMailFromDomainAttributes",
"ses:getIdentityNotificationAttributes",
"ses:getIdentityPolicies",
"ses:getIdentityVerificationAttributes",
"ses:getImportJob",
"ses:getSendQuota",
"ses:getSendStatistics",
"ses:listConfigurationSets",
"ses:listContactLists",
"ses:listContacts",
"ses:listCustomVerificationEmailTemplates",
"ses:listDedicatedIpPools",
"ses:listDeliverabilityTestReports",
"ses:listDomainDeliverabilityCampaigns",
"ses:listEmailIdentities",
"ses:listEmailTemplates",
"ses:listIdentities",
"ses:listIdentityPolicies",
"ses:listImportJobs",
"ses:listReceiptFilters",
"ses:listReceiptRuleSets",
"ses:listRecommendations",
"ses:listTagsForResource",
"ses:listTemplates",
```



```
"ses:listVerifiedEmailAddresses",
"shield:describeAttack",
"shield:describeProtection",
"shield:describeSubscription",
"shield:listAttacks",
"shield:listProtections",
"sms-voice:getConfigurationSetEventDestinations",
"sms:getConnectors",
"sms:getReplicationJobs",
"sms:getReplicationRuns",
"sms:getServers",
"snowball:describeAddress",
"snowball:describeAddresses",
"snowball:describeJob",
"snowball:getSnowballUsage",
"snowball:listJobs",
"snowball:listServiceVersions",
"sns:checkIfPhoneNumberIsOptedOut",
"sns:getDataProtectionPolicy",
"sns:getEndpointAttributes",
"sns:getPlatformApplicationAttributes",
"sns:getSMSAttributes",
"sns:getSMSSandboxAccountStatus",
"sns:getSubscriptionAttributes",
"sns:getTopicAttributes",
"sns:listEndpointsByPlatformApplication",
"sns:listOriginationNumbers",
"sns:listPhoneNumbersOptedOut",
"sns:listPlatformApplications",
"sns:listSMSSandboxPhoneNumbers",
"sns:listSubscriptions",
"sns:listSubscriptionsByTopic",
"sns:listTopics",
"sqs:getQueueAttributes",
"sqs:getQueueUrl",
"sqs:listDeadLetterSourceQueues",
"sqs:listQueues",
"ssm-contacts:describeEngagement",
"ssm-contacts:describePage",
"ssm-contacts:getContact",
"ssm-contacts:getContactChannel",
"ssm-contacts:getContactPolicy",
"ssm-contacts:getRotation",
"ssm-contacts:getRotationOverride",
```

```
"ssm-contacts:listContactChannels",
"ssm-contacts:listContacts",
"ssm-contacts:listEngagements",
"ssm-contacts:listPageReceipts",
"ssm-contacts:listPageResolutions",
"ssm-contacts:listPagesByContact",
"ssm-contacts:listPagesByEngagement",
"ssm-contacts:listPreviewRotationShifts",
"ssm-contacts:listRotationOverrides",
"ssm-contacts:listRotations",
"ssm-contacts:listRotationShifts",
"ssm-incidents:getIncidentRecord",
"ssm-incidents:getReplicationSet",
"ssm-incidents:getResourcePolicies",
"ssm-incidents:getResponsePlan",
"ssm-incidents:getTimelineEvent",
"ssm-incidents:listIncidentRecords",
"ssm-incidents:listRelatedItems",
"ssm-incidents:listReplicationSets",
"ssm-incidents:listResponsePlans",
"ssm-incidents:listTimelineEvents",
"ssm-sap:getApplication",
"ssm-sap:getComponent",
"ssm-sap:getDatabase",
"ssm-sap:getOperation",
"ssm-sap:getResourcePermission",
"ssm-sap:listApplications",
"ssm-sap:listComponents",
"ssm-sap:listDatabases",
"ssm-sap:listOperations",
"ssm:describeActivations",
"ssm:describeAssociation",
"ssm:describeAssociationExecutions",
"ssm:describeAssociationExecutionTargets",
"ssm:describeAutomationExecutions",
"ssm:describeAutomationStepExecutions",
"ssm:describeAvailablePatches",
"ssm:describeDocument",
"ssm:describeDocumentPermission",
"ssm:describeEffectiveInstanceAssociations",
"ssm:describeEffectivePatchesForPatchBaseline",
"ssm:describeInstanceAssociationsStatus",
"ssm:describeInstanceInformation",
"ssm:describeInstancePatches",
```

```
"ssm:describeInstancePatchStates",
"ssm:describeInstancePatchStatesForPatchGroup",
"ssm:describeInventoryDeletions",
"ssm:describeMaintenanceWindowExecutions",
"ssm:describeMaintenanceWindowExecutionTaskInvocations",
"ssm:describeMaintenanceWindowExecutionTasks",
"ssm:describeMaintenanceWindows",
"ssm:describeMaintenanceWindowSchedule",
"ssm:describeMaintenanceWindowsForTarget",
"ssm:describeMaintenanceWindowTargets",
"ssm:describeMaintenanceWindowTasks",
"ssm:describeOpsItems",
"ssm:describeParameters",
"ssm:describePatchBaselines",
"ssm:describePatchGroups",
"ssm:describePatchGroupState",
"ssm:describePatchProperties",
"ssm:describeSessions",
"ssm:getAutomationExecution",
"ssm:getCalendarState",
"ssm:getCommandInvocation",
"ssm:getConnectionStatus",
"ssm:getDefaultPatchBaseline",
"ssm:getDeployablePatchSnapshotForInstance",
"ssm:getInventorySchema",
"ssm:getMaintenanceWindow",
"ssm:getMaintenanceWindowExecution",
"ssm:getMaintenanceWindowExecutionTask",
"ssm:getMaintenanceWindowExecutionTaskInvocation",
"ssm:getMaintenanceWindowTask",
"ssm:getOpsItem",
"ssm:getOpsMetadata",
"ssm:getOpsSummary",
"ssm:getPatchBaseline",
"ssm:getPatchBaselineForPatchGroup",
"ssm:getResourcePolicies",
"ssm:getServiceSetting",
"ssm:listAssociations",
"ssm:listAssociationVersions",
"ssm:listCommandInvocations",
"ssm:listCommands",
"ssm:listComplianceItems",
"ssm:listComplianceSummaries",
"ssm:listDocuments",
```

```
"ssm:listDocumentMetadataHistory",
"ssm:listDocumentVersions",
"ssm:listOpsItemEvents",
"ssm:listOpsItemRelatedItems",
"ssm:listOpsMetadata",
"ssm:listResourceComplianceSummaries",
"ssm:listResourceDataSync",
"ssm:listTagsForResource",
"sso:describeApplicationAssignment",
"sso:describeApplicationProvider",
"sso:describeApplication",
"sso:describeInstance",
"sso:describeTrustedTokenIssuer",
"sso:getApplicationAccessScope",
"sso:getApplicationAssignmentConfiguration",
"sso:getApplicationAuthenticationMethod",
"sso:getApplicationGrant",
"sso:getApplicationInstance",
"sso:getApplicationTemplate",
"sso:getManagedApplicationInstance",
"sso:getSharedSsoConfiguration",
"sso:listApplicationAccessScopes",
"sso:listApplicationAssignments",
"sso:listApplicationAuthenticationMethods",
"sso:listApplicationGrants",
"sso:listApplicationInstances",
"sso:listApplicationProviders",
"sso:listApplications",
"sso:listApplicationTemplates",
"sso:listDirectoryAssociations",
"sso:listInstances",
"sso:listProfileAssociations",
"sso:listTrustedTokenIssuers",
"states:describeActivity",
"states:describeExecution",
"states:describeMapRun",
"states:describeStateMachine",
"states:describeStateMachineAlias",
"states:describeStateMachineForExecution",
"states:getExecutionHistory",
"states:listActivities",
"states:listExecutions",
"states:listMapRuns",
"states:listStateMachineAliases",
```

```
"states:listStateMachines",
"states:listStateMachineVersions",
"storagegateway:describeBandwidthRateLimit",
"storagegateway:describeCache",
"storagegateway:describeCachediSCSIVolumes",
"storagegateway:describeFileSystemAssociations",
"storagegateway:describeGatewayInformation",
"storagegateway:describeMaintenanceStartTime",
"storagegateway:describeNFSFileShares",
"storagegateway:describeSMBFileShares",
"storagegateway:describeSMBSettings",
"storagegateway:describeSnapshotSchedule",
"storagegateway:describeStorediSCSIVolumes",
"storagegateway:describeTapeArchives",
"storagegateway:describeTapeRecoveryPoints",
"storagegateway:describeTapes",
"storagegateway:describeUploadBuffer",
"storagegateway:describeVTLDevices",
"storagegateway:describeWorkingStorage",
"storagegateway:listAutomaticTapeCreationPolicies",
"storagegateway:listFileShares",
"storagegateway:listFileSystemAssociations",
"storagegateway:listGateways",
"storagegateway:listLocalDisks",
"storagegateway:listTagsForResource",
"storagegateway:listTapes",
"storagegateway:listVolumeInitiators",
"storagegateway:listVolumeRecoveryPoints",
"storagegateway:listVolumes",
"swf:countClosedWorkflowExecutions",
"swf:countOpenWorkflowExecutions",
"swf:countPendingActivityTasks",
"swf:countPendingDecisionTasks",
"swf:describeActivityType",
"swf:describeDomain",
"swf:describeWorkflowExecution",
"swf:describeWorkflowType",
"swf:getWorkflowExecutionHistory",
"swf:listActivityTypes",
"swf:listClosedWorkflowExecutions",
"swf:listDomains",
"swf:listOpenWorkflowExecutions",
"swf:listWorkflowTypes",
"synthetics:describeCanaries",
```

```
"synthetics:describeCanariesLastRun",
"synthetics:describeRuntimeVersions",
"synthetics:getCanary",
"synthetics:getCanaryRuns",
"synthetics:getGroup",
"synthetics:listAssociatedGroups",
"synthetics:listGroupResources",
"synthetics:listGroups",
"tiros:createQuery",
"tiros:getQueryAnswer",
"tiros:getQueryExplanation",
"transcribe:describeLanguageModel",
"transcribe:getCallAnalyticsCategory",
"transcribe:getCallAnalyticsJob",
"transcribe:getMedicalTranscriptionJob",
"transcribe:getMedicalVocabulary",
"transcribe:getTranscriptionJob",
"transcribe:getVocabulary",
"transcribe:getVocabularyFilter",
"transcribe:listCallAnalyticsCategories",
"transcribe:listCallAnalyticsJobs",
"transcribe:listLanguageModels",
"transcribe:listMedicalTranscriptionJobs",
"transcribe:listMedicalVocabularies",
"transcribe:listTranscriptionJobs",
"transcribe:listVocabularies",
"transcribe:listVocabularyFilters",
"transfer:describeAccess",
"transfer:describeAgreement",
"transfer:describeConnector",
"transfer:describeExecution",
"transfer:describeProfile",
"transfer:describeServer",
"transfer:describeUser",
"transfer:describeWorkflow",
"transfer:listAccesses",
"transfer:listAgreements",
"transfer:listConnectors",
"transfer:listExecutions",
"transfer:listHostKeys",
"transfer:listProfiles",
"transfer:listServers",
"transfer:listTagsForResource",
"transfer:listUsers",
```

```
"transfer:listWorkflows",
"transfer:sendWorkflowStepState",
"trustedadvisor:getOrganizationRecommendation",
"trustedadvisor:getRecommendation",
"trustedadvisor:listChecks",
"trustedadvisor:listOrganizationRecommendationAccounts",
"trustedadvisor:listOrganizationRecommendationResources",
"trustedadvisor:listOrganizationRecommendations",
"trustedadvisor:listRecommendationResources",
"trustedadvisor:listRecommendations",
"verifiedpermissions:getIdentitySource",
"verifiedpermissions:getPolicy",
"verifiedpermissions:getPolicyStore",
"verifiedpermissions:getPolicyTemplate",
"verifiedpermissions:getSchema",
"verifiedpermissions:listIdentitySources",
"verifiedpermissions:listPolicies",
"verifiedpermissions:listPolicyStores",
"verifiedpermissions:listPolicyTemplates",
"vpc-lattice:getAccessLogSubscription",
"vpc-lattice:getAuthPolicy",
"vpc-lattice:getListener",
"vpc-lattice:getResourcePolicy",
"vpc-lattice:getRule",
"vpc-lattice:getService",
"vpc-lattice:getServiceNetwork",
"vpc-lattice:getServiceNetworkServiceAssociation",
"vpc-lattice:getServiceNetworkVpcAssociation",
"vpc-lattice:getTargetGroup",
"vpc-lattice:listAccessLogSubscriptions",
"vpc-lattice:listListeners",
"vpc-lattice:listRules",
"vpc-lattice:listServiceNetworks",
"vpc-lattice:listServiceNetworkServiceAssociations",
"vpc-lattice:listServiceNetworkVpcAssociations",
"vpc-lattice:listServices",
"vpc-lattice:listTargetGroups",
"vpc-lattice:listTargets",
"waf-regional:getByteMatchSet",
"waf-regional:getChangeTokenStatus",
"waf-regional:getGeoMatchSet",
"waf-regional:getIPSet",
"waf-regional:getLoggingConfiguration",
"waf-regional:getRateBasedRule",
```

```
"waf-regional:getRegexMatchSet",
"waf-regional:getRegexPatternSet",
"waf-regional:getRule",
"waf-regional:getRuleGroup",
"waf-regional:getSqlInjectionMatchSet",
"waf-regional:getWebACL",
"waf-regional:getWebACLForResource",
"waf-regional:listActivatedRulesInRuleGroup",
"waf-regional:listByteMatchSets",
"waf-regional:listGeoMatchSets",
"waf-regional:listIPSets",
"waf-regional:listLoggingConfigurations",
"waf-regional:listRateBasedRules",
"waf-regional:listRegexMatchSets",
"waf-regional:listRegexPatternSets",
"waf-regional:listResourcesForWebACL",
"waf-regional:listRuleGroups",
"waf-regional:listRules",
"waf-regional:listSqlInjectionMatchSets",
"waf-regional:listWebACLs",
"waf:getByteMatchSet",
"waf:getChangeTokenStatus",
"waf:getGeoMatchSet",
"waf:getIPSet",
"waf:getLoggingConfiguration",
"waf:getRateBasedRule",
"waf:getRegexMatchSet",
"waf:getRegexPatternSet",
"waf:getRule",
"waf:getRuleGroup",
"waf:getSampledRequests",
"waf:getSizeConstraintSet",
"waf:getSqlInjectionMatchSet",
"waf:getWebACL",
"waf:getXssMatchSet",
"waf:listActivatedRulesInRuleGroup",
"waf:listByteMatchSets",
"waf:listGeoMatchSets",
"waf:listIPSets",
"waf:listLoggingConfigurations",
"waf:listRateBasedRules",
"waf:listRegexMatchSets",
"waf:listRegexPatternSets",
"waf:listRuleGroups",
```



```
"waf:listRules",
"waf:listSizeConstraintSets",
"waf:listSqlInjectionMatchSets",
"waf:listWebACLs",
"waf:listXssMatchSets",
"wafv2:checkCapacity",
"wafv2:describeManagedRuleGroup",
"wafv2:getIPSet",
"wafv2:getLoggingConfiguration",
"wafv2:getPermissionPolicy",
"wafv2:getRateBasedStatementManagedKeys",
"wafv2:getRegexPatternSet",
"wafv2:getRuleGroup",
"wafv2:getSampledRequests",
"wafv2:getWebACL",
"wafv2:getWebACLForResource",
"wafv2:listAvailableManagedRuleGroups",
"wafv2:listIPSets",
"wafv2:listLoggingConfigurations",
"wafv2:listRegexPatternSets",
"wafv2:listResourcesForWebACL",
"wafv2:listRuleGroups",
"wafv2:listTagsForResource",
"wafv2:listWebACLs",
"workdocs:checkAlias",
"workdocs:describeAvailableDirectories",
"workdocs:describeInstances",
"workmail:describeGroup",
"workmail:describeOrganization",
"workmail:describeResource",
"workmail:describeUser",
"workmail:listAliases",
"workmail:listGroupMembers",
"workmail:listGroups",
"workmail:listMailboxPermissions",
"workmail:listOrganizations",
"workmail:listResourceDelegates",
"workmail:listResources",
"workmail:listUsers",
"workspaces-web:getBrowserSettings",
"workspaces-web:getIdentityProvider",
"workspaces-web:getNetworkSettings",
"workspaces-web:getPortal",
"workspaces-web:getPortalServiceProviderMetadata",
```

```

    "workspaces-web:getTrustStoreCertificate",
    "workspaces-web:getUserSettings",
    "workspaces-web:listBrowserSettings",
    "workspaces-web:listIdentityProviders",
    "workspaces-web:listNetworkSettings",
    "workspaces-web:listPortals",
    "workspaces-web:listTagsForResource",
    "workspaces-web:listTrustStoreCertificates",
    "workspaces-web:listTrustStores",
    "workspaces-web:listUserSettings",
    "workspaces:describeAccount",
    "workspaces:describeAccountModifications",
    "workspaces:describeIpGroups",
    "workspaces:describeTags",
    "workspaces:describeWorkspaceBundles",
    "workspaces:describeWorkspaceDirectories",
    "workspaces:describeWorkspaceImages",
    "workspaces:describeWorkspaces",
    "workspaces:describeWorkspacesConnectionStatus",
    "xray:getEncryptionConfig",
    "xray:getGroup",
    "xray:getGroups",
    "xray:getSamplingRules",
    "xray:listResourcePolicies"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
}
],
"Version" : "2012-10-17"
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

설명: AWS Systems Manager (SSM) 에게 AWS 계정 정보를 검색할 수 있는 권한을 부여합니다.

AWSSystemsManagerAccountDiscoveryServicePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 24일, 17:21 UTC
- 편집된 시간: 2022년 10월 17일, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSystemsManagerChangeManagementServicePolicy

설명: AWS Systems Manager 변경 관리 프레임워크에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

AWSSystemsManagerChangeManagementServicePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 7일, 22:21 UTC
- 편집된 시간: 2020년 12월 7일, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSystemsManagerForSAPFullAccess

설명: SAP용 AWS Systems Manager 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSSystemsManagerForSAPFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSystemsManagerForSAPFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 17일, 02:11 UTC
- 편집된 시간: 2022년 11월 18일, 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSystemsManagerForSAPReadOnlyAccess

설명: SAP용 AWS Systems Manager 서비스에 대한 읽기 전용 액세스 권한을 제공합니다.

AWSSystemsManagerForSAPReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSystemsManagerForSAPReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 17일, 02:11 UTC
- 편집된 시간: 2022년 11월 17일, 02:11 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

설명: 관련 작업을 관리하기 OpsData 위한 SSM 탐색기의 IAM 역할

AWSSystemsManagerOpsDataSyncServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 26일, 20:42 UTC
- 편집된 시간: 2023년 6월 28일, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }  
  }  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxAssetServerPolicy

설명: 이 정책은 AWS 포털 에셋 서버에 정상적인 운영에 필요한 권한을 부여합니다.

AWSThinkboxAssetServerPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAssetServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:18 UTC
- 편집된 시간: 2020년 5월 27일, 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxAWSPortalAdminPolicy

설명: 이 정책은 AWS Thinkbox의 Deadline 소프트웨어에 AWS 포털 관리에 필요한 여러 AWS 서비스에 대한 전체 액세스 권한을 부여합니다. 여기에는 여러 EC2 리소스 유형에 대한 임의의 태그를 생성할 수 있는 액세스가 포함됩니다.

AWSThinkboxAWSPortalAdminPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAWSPortalAdminPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:41 UTC
- 편집 시간: 2024년 4월 12일 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:rds-tls-pw*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxAWSPortalGatewayPolicy

설명: 이 정책은 AWS Portal Gateway 컴퓨터에 정상 작동에 필요한 권한을 부여합니다.

AWSThinkboxAWSPortalGatewayPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAWSPortalGatewayPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:05 UTC
- 편집된 시간: 2020년 6월 30일, 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "dynamodb:Scan",
    "Resource" : [
      "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*/gateway_certs/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)

- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxAWSPortalWorkerPolicy

설명: 이 정책은 AWS 포털의 Deadline Worker에게 정상적인 운영에 필요한 권한을 부여합니다.

AWSThinkboxAWSPortalWorkerPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAWSPortalWorkerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:15 UTC
- 편집된 시간: 2020년 12월 7일, 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

설명: AWS Thinkbox의 데드라인 리소스 트래커 운영에 필요한 권한을 부여합니다. 여기에는 및 를 포함한 일부 EC2 작업에 대한 전체 액세스 권한이 포함됩니다. DeleteFleets CancelSpotFleetRequests

AWSThinkboxDeadlineResourceTrackerAccessPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineResourceTrackerAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:25 UTC
- 편집된 시간: 2020년 5월 27일, 19:25 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineResourceTrackerAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

설명: AWS Thinkbox의 데드라인 리소스 트래커를 생성, 삭제 및 관리하는 데 필요한 권한을 부여합니다.

AWSThinkboxDeadlineResourceTrackerAdminPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineResourceTrackerAdminPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:29 UTC
- 편집 시간: 2024년 4월 12일 20:55 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineResourceTrackerAdminPolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

설명: AWS Thinkbox의 데드라인 스팟 이벤트 플러그인에 필요한 권한을 부여합니다. 여기에는 스팟 풀릿을 요청, 수정 및 취소할 수 있는 권한과 제한된 PassRole 권한이 포함됩니다.

AWSThinkboxDeadlineSpotEventPluginAdminPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineSpotEventPluginAdminPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:38 UTC
- 편집된 시간: 2020년 5월 27일, 19:38 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginAdminPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

설명: AWS Thinkbox Deadline 스팟 이벤트 플러그인 워커 소프트웨어를 실행하는 EC2 인스턴스에 필요한 권한을 부여합니다.

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineSpotEventPluginWorkerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:35 UTC
- 편집된 시간: 2020년 12월 7일, 23:31 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTransferConsoleFullAccess

설명: 다음을 통해 AWS 전송에 대한 전체 액세스 권한을 제공합니다. AWS Management Console AWSTransferConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 14일, 19:33 UTC
- 편집된 시간: 2020년 12월 14일, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```



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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTransferFullAccess

설명: AWS 전송 서비스에 대한 전체 액세스 권한을 제공합니다.

AWSTransferFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 14일, 19:37 UTC
- 편집된 시간: 2020년 12월 14일, 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTransferLoggingAccess

설명: 전체 액세스 권한을 AWS 전송하여 로그 스트림 및 그룹을 생성하고 계정에 로그 이벤트를 추가할 수 있습니다.

AWSTransferLoggingAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferLoggingAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 1월 14일, 15:32 UTC

- 편집된 시간: 2019년 1월 14일, 15:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTransferReadOnlyAccess

설명: AWS 전송 서비스에 대한 읽기 전용 액세스를 제공합니다.

AWSTransferReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 27일, 17:54 UTC
- 편집된 시간: 2020년 8월 27일, 17:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",

```

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTrustedAdvisorPriorityFullAccess

설명: AWS Trusted Advisor 우선 순위에 대한 전체 액세스 권한을 제공합니다. 또한 이 정책을 통해 사용자는 Trusted Advisor를 AWS Organizations의 신뢰할 수 있는 서비스로 추가하고 Trusted Advisor Priority의 위임된 관리자 계정을 지정할 수 있습니다.

AWSTrustedAdvisorPriorityFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSTrustedAdvisorPriorityFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 16:08 UTC
- 편집된 시간: 2022년 8월 16일, 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

설명: AWS Trusted Advisor 우선 순위에 대한 읽기 전용 액세스를 제공합니다. 여기에는 위임된 관리자 계정을 볼 수 있는 권한이 포함됩니다.

AWSTrustedAdvisorPriorityReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTrustedAdvisorPriorityReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 16:35 UTC
- 편집된 시간: 2022년 8월 16일, 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTrustedAdvisorReportingServiceRolePolicy

설명: Trusted Advisor 다중 계정 보고 서비스 정책

AWSTrustedAdvisorReportingServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 19일, 17:41 UTC
- 편집된 시간: 2023년 2월 28일, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSTrustedAdvisorServiceRolePolicy

설명: AWS Trusted Advisor 서비스에 액세스하여 비용을 절감하고 성능을 높이며 사용자 AWS 환경의 보안을 개선할 수 있습니다.

AWSTrustedAdvisorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 2월 22일, 21:24 UTC
- 편집 시간: 2024년 6월 11일 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSUserNotificationsServiceLinkedRolePolicy

설명: AWS 사용자 알림이 사용자를 대신하여 AWS 서비스에 전화를 걸 수 있도록 허용합니다.

AWSUserNotificationsServiceLinkedRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 19일, 13:28 UTC
- 편집된 시간: 2023년 4월 19일, 13:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVendorInsightsAssessorFullAccess

설명: 사용 권한이 있는 공급업체 인사이트 리소스를 보고 공급업체 인사이트 구독을 관리할 수 있는 전체 액세스 권한을 제공합니다.

AWSVendorInsightsAssessorFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsAssessorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC

- 편집된 시간: 2022년 12월 1일, 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVendorInsightsAssessorReadOnly

설명: 권한이 있는 Vendor Insights 리소스를 볼 수 있는 읽기 전용 액세스 권한을 제공합니다.

AWSVendorInsightsAssessorReadOnly [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsAssessorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2022년 12월 1일, 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVendorInsightsVendorFullAccess

설명: 벤더 인사이트 리소스를 만들고 관리하기 위한 전체 액세스 권한을 제공합니다.

AWSVendorInsightsVendorFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsVendorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2023년 10월 19일, 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVendorInsightsVendorReadOnly

설명: 벤더 인사이트 리소스를 볼 수 있는 읽기 전용 액세스 권한을 제공합니다.

AWSVendorInsightsVendorReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsVendorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2022년 12월 1일, 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVpcLatticeServiceRolePolicy

설명: VPC Lattice가 사용자 대신 AWS 리소스에 액세스할 수 있도록 허용합니다.

AWSVpcLatticeServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 30일, 20:47 UTC
- 편집된 시간: 2022년 11월 30일, 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVPCS2SVpnServiceRolePolicy

설명: Site-to-Site VPN이 VPN 연결과 관련된 리소스를 만들고 관리할 수 있도록 허용합니다.

AWSVPCS2SVpnServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 6일, 14:13 UTC
- 편집된 시간: 2019년 8월 6일, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVPCTransitGatewayServiceRolePolicy

설명: VPC Transit Gateway에서 Transit Gateway VPC 첨부 파일에 필요한 리소스를 만들고 관리할 수 있도록 허용합니다.

AWSVPCTransitGatewayServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 16:21 UTC
- 편집된 시간: 2021년 4월 15일, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSVPCVerifiedAccessServiceRolePolicy

설명: AWS Verified Access 서비스가 사용자를 대신하여 엔드포인트를 프로비저닝할 수 있도록 하는 정책

AWSVPCVerifiedAccessServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 29일, 03:35 UTC
- 편집 시간: 2023년 11월 17일, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWAFConsoleFullAccess

설명: 를 통해 AWS WAF에 대한 전체 액세스를 제공합니다. AWS Management Console이 정책은 Amazon CloudFront 배포를 나열하고 업데이트할 수 있는 권한, AWS Elastic Load Balancing에서 로

드 밸런서를 볼 수 있는 권한, Amazon API Gateway REST API 및 단계를 볼 수 있는 권한, Amazon CloudWatch 지표를 나열하고 볼 수 있는 권한, 계정 내에서 활성화된 지역을 볼 수 있는 권한도 부여한다는 점에 유의하십시오.

AWSWAFConsoleFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 6일, 18:38 UTC
- 편집된 시간: 2023년 6월 5일, 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWAFConsoleReadOnlyAccess

설명: 를 통해 AWS WAF에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console이 정책은 Amazon CloudFront 배포를 나열할 권한, AWS Elastic Load Balancing에서 로드 밸런서를 볼 수 있는 권한, Amazon API Gateway REST API 및 단계를 볼 수 있는 권한, Amazon CloudWatch 지표를 나열하고 볼 수 있는 권한, 계정 내에서 활성화된 지역을 볼 수 있는 권한도 부여한다는 점에 유의하십시오.

AWSWAFConsoleReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 6일, 18:43 UTC
- 편집된 시간: 2023년 6월 5일, 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWAFFullAccess

설명: AWS WAF 작업에 대한 전체 액세스 권한을 제공합니다.

AWSWAFFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 6일, 20:44 UTC
- 편집된 시간: 2023년 6월 5일, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
]

```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWAFReadOnlyAccess

설명: AWS WAF 작업에 대한 읽기 전용 액세스를 제공합니다.

AWSWAFReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 6일, 20:43 UTC
- 편집된 시간: 2023년 6월 5일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

설명: 고객을 대신하여 리소스와 관련된 AWS 서비스 및 WellArchitected 리소스에 액세스할 수 있습니다. WellArchitected

AWSWellArchitectedDiscoveryServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 26일, 18:36 UTC
- 편집된 시간: 2023년 4월 26일, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicelog:ListAssociatedResources",
    "servicelog:GetApplication",
    "servicelog>CreateAttributeGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicelog:AssociateAttributeGroup",
    "servicelog:DisassociateAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicelog:*:*:/applications/*",
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicelog:UpdateAttributeGroup",
    "servicelog>DeleteAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

설명: Well-Architected가 사용자 대신 Organizations에 액세스할 수 있도록 허용합니다.

AWSWellArchitectedOrganizationsServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 23일, 17:15 UTC
- 편집된 시간: 2022년 7월 25일, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSWickrFullAccess

설명: 이 정책은 에 따른 Wickr 관리 기능을 포함하여 Wickr 서비스에 전체 관리 권한을 부여합니다.
AWS Management Console

AWSWickrFullAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSWickrFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 20:36 UTC
- 편집된 시간: 2022년 11월 27일, 20:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSXrayCrossAccountSharingConfiguration

설명: Observability Access Manager 링크를 관리하고 X-Ray 추적 공유를 설정하는 기능을 제공합니다.

AWSXrayCrossAccountSharingConfiguration [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayCrossAccountSharingConfiguration를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:46 UTC
- 편집된 시간: 2022년 11월 27일, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSXRayDaemonWriteAccess

설명: AWS X-Ray 데몬이 원시 추적 세그먼트 데이터를 서비스의 API로 중계하고 X-Ray SDK에서 사용할 샘플링 데이터 (규칙, 대상 등) 를 검색할 수 있도록 허용합니다.

AWSXRayDaemonWriteAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 AWSXRayDaemonWriteAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 8월 28일, 23:00 UTC
- 편집 시간: 2024년 2월 13일 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSXrayFullAccess

설명: AWS X-Ray 전체 액세스 관리형 정책

AWSXrayFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:30 UTC
- 편집 시간: 2024년 4월 11일 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSXrayReadOnlyAccess

설명: AWS X-Ray 읽기 전용 관리형 정책

AWSXrayReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:27 UTC
- 편집 시간: 2024년 2월 14일 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSXrayWriteOnlyAccess

설명: AWS X-Ray 쓰기 전용 관리형 정책

AWSXrayWriteOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayWriteOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:19 UTC
- 편집된 시간: 2018년 8월 28일, 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

설명: ARC 구역 교대 연습 실행에 대한 관리 액세스 권한과 연습 실행을 모니터링하기 위한 CloudWatch 경보 상태에 대한 액세스를 제공합니다.

AWSZonalAutoshiftPracticeRunSLRPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2023년 11월 29일 17:34 UTC
- 편집 시간: 2023년 11월 29일 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

BatchServiceRolePolicy

설명: Amazon EC2 및 Amazon ECS 리소스를 비롯한 필수 리소스를 관리하기 위한 AWS Batch 서비스에 대한 액세스를 제공합니다.

BatchServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 3월 10일, 06:55 UTC
- 편집 시간: 2023년 12월 5일, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Billing

설명: 청구 및 비용 관리 권한을 부여합니다. 여기에는 계정 사용량 보기, 예산 및 결제 방법 보기 및 수정이 포함됩니다.

Billing [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 Billing를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:33 UTC
- 편집 시간: 2024년 5월 23일 23:26 UTC
- ARN: arn:aws:iam::aws:policy/job-function/Billing

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CertificateManagerServiceRolePolicy

설명: Amazon 인증서 관리자 서비스 역할 정책

CertificateManagerServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 25일, 17:56 UTC
- 편집된 시간: 2020년 6월 25일, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ClientVPNServiceConnectionsRolePolicy

설명: Client VPN이 AWS 클라이언트 VPN 엔드포인트 연결을 관리할 수 있도록 하는 정책입니다.

ClientVPNServiceConnectionsRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2020년 8월 12일, 19:48 UTC
- 편집된 시간: 2020년 8월 12일, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ClientVPNServiceRolePolicy

설명: Client VPN이 AWS 클라이언트 VPN 엔드포인트를 관리할 수 있도록 하는 정책입니다.

ClientVPNServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 12월 10일, 21:20 UTC
- 편집된 시간: 2020년 8월 12일, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

설명: CloudFormation StackSets (조직 마스터 계정) 의 서비스 역할

CloudFormationStackSetsOrgAdminServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 10일, 00:20 UTC
- 편집된 시간: 2019년 12월 10일, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

설명: CloudFormation StackSets (조직 구성원 계정) 의 서비스 역할

CloudFormationStackSetsOrgMemberServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 9일, 23:52 UTC
- 편집된 시간: 2019년 12월 9일, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudFrontFullAccess

설명: CloudFront 콘솔에 대한 전체 액세스 권한과 함께 를 통해 Amazon S3 버킷을 나열할 수 있는 AWS Management Console 기능을 제공합니다.

CloudFrontFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudFrontFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 1월 4일 16:56 UTC
- ARN: arn:aws:iam::aws:policy/CloudFrontFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cfffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
```

```
    "Resource" : "arn:aws:kinesis:*:*:*"
  },
  {
    "Sid" : "cfflistroles",
    "Action" : [
      "iam:ListRoles"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam:*:*:*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudFrontReadOnlyAccess

설명: 를 통해 CloudFront 배포 구성 정보 및 목록 배포에 액세스할 수 있습니다. AWS Management Console

CloudFrontReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudFrontReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 1월 4일 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudHSMServiceRolePolicy

설명: CloudHSM에서 사용하거나 관리하는 AWS 리소스에 액세스할 수 있습니다.

CloudHSMServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 6일, 19:12 UTC
- 편집된 시간: 2017년 11월 6일, 19:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",

```

```
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:*"
  ]
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudSearchFullAccess

설명: Amazon CloudSearch 구성 서비스에 대한 전체 액세스 권한을 제공합니다.

CloudSearchFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudSearchFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudSearchReadOnlyAccess

설명: Amazon CloudSearch 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

CloudSearchReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudSearchReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudTrailServiceRolePolicy

설명: 권한 정책: CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 10월 24일, 21:21 UTC
- 편집 시간: 2023년 11월 27일, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
    }
  }
}

```

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatch-CrossAccountAccess

설명: 계정 간, CloudWatch 지역 간 데이터를 표시하기 위해 현재 계정을 대신하여 원격 계정에서 CrossAccountSharing 역할을 맡을 수 CloudWatch 있습니다.

CloudWatch-CrossAccountAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 7월 23일, 09:59 UTC
- 편집된 시간: 2019년 7월 23일, 09:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchActionsEC2Access

설명: CloudWatch 경보 및 지표와 EC2 메타데이터에 대한 읽기 전용 액세스를 제공합니다. EC2 인스턴스를 중지, 종료 및 재부팅할 수 있는 액세스를 제공합니다.

CloudWatchActionsEC2Access [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchActionsEC2Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 7일, 00:00 UTC
- 편집된 시간: 2015년 7월 7일, 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchAgentAdminPolicy

설명: 사용하려면 전체 권한이 필요합니다 AmazonCloudWatchAgent.

CloudWatchAgentAdminPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchAgentAdminPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 00:52 UTC
- 편집 시간: 2024년 2월 5일 20:59 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchAgentServerPolicy

설명: AmazonCloudWatchAgent 서버에서 사용하는 데 필요한 권한

CloudWatchAgentServerPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchAgentServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 01:06 UTC
- 편집 시간: 2024년 2월 6일 16:37 UTC

- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchApplicationInsightsFullAccess

설명: CloudWatch 애플리케이션 인사이트 및 필수 종속성에 대한 전체 액세스 권한을 제공합니다.

CloudWatchApplicationInsightsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchApplicationInsightsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 24일, 18:44 UTC
- 편집된 시간: 2022년 1월 25일, 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
    }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchApplicationInsightsReadOnlyAccess

설명: CloudWatch 애플리케이션 인사이트에 대한 읽기 전용 액세스를 제공합니다.

CloudWatchApplicationInsightsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchApplicationInsightsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 24일, 18:48 UTC
- 편집된 시간: 2020년 11월 24일, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

설명: Cloudwatch 애플리케이션 인사이트 서비스 연계 역할 정책

CloudwatchApplicationInsightsServiceLinkedRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 12월 1일, 16:22 UTC
- 편집된 시간: 2023년 5월 11일, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

정책 버전

정책 버전: v24(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchApplicationSignalsFullAccess

설명: CloudWatch Application Signal 서비스에 대한 전체 액세스 권한과 이 서비스를 사용하고 운영하는 데 필요한 종속성에 대한 범위 지정 액세스를 제공합니다.

CloudWatchApplicationSignalsFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchApplicationSignalsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 6월 6일 22:50 UTC
- 편집 시간: 2024년 6월 6일 22:50 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchApplicationSignalsReadOnlyAccess

설명: CloudWatch Application Signal 서비스에 대한 읽기 전용 액세스와 이 서비스를 사용하는 데 필요한 종속성에 대한 범위 지정 액세스를 제공합니다.

CloudWatchApplicationSignalsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchApplicationSignalsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 6월 6일 22:48 UTC
- 편집 시간: 2024년 6월 6일 22:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:BatchGetRunMetricDefinitions",
    "rum:GetAppMonitor",
    "rum:GetAppMonitorData",
    "rum:ListAppMonitors"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
  "Effect" : "Allow",
  "Action" : [
    "xray:GetTraceSummaries"
  ],
  "Resource" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchApplicationSignalsServiceRolePolicy

설명: 정책은 CloudWatch 애플리케이션 시그널에 다른 관련 AWS 서비스로부터 모니터링 및 태깅 데이터를 수집할 수 있는 권한을 부여합니다.

CloudWatchApplicationSignalsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 9일, 18:09 UTC
- 편집 시간: 2024년 4월 26일 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchAutomaticDashboardsAccess

설명: Lambda 함수와 같은 객체의 콘텐츠를 포함하여 CloudWatch 자동 대시보드를 표시하는 데 사용되는 비 CloudWatch API에 대한 액세스를 제공합니다.

CloudWatchAutomaticDashboardsAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchAutomaticDashboardsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 23일, 10:01 UTC
- 편집된 시간: 2021년 4월 20일, 13:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchCrossAccountSharingConfiguration

설명: Observability Access Manager 링크를 관리하고 리소스 공유를 설정하는 기능을 제공합니다.
CloudWatch

CloudWatchCrossAccountSharingConfiguration [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchCrossAccountSharingConfiguration를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 14:01 UTC
- 편집된 시간: 2022년 11월 27일, 14:01 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchEventsBuiltInTargetExecutionAccess

설명: Amazon CloudWatch Events에 내장된 대상이 사용자를 대신하여 EC2 작업을 수행할 수 있도록 합니다.

CloudWatchEventsBuiltInTargetExecutionAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchEventsBuiltInTargetExecutionAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 14일, 18:35 UTC
- 편집된 시간: 2016년 1월 14일, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchEventsFullAccess

설명: Amazon CloudWatch 이벤트에 대한 전체 액세스 권한을 제공합니다.

CloudWatchEventsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchEventsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2016년 1월 14일, 18:37 UTC
- 편집된 시간: 2022년 12월 1일, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchEventsInvocationAccess

설명: Amazon CloudWatch Events가 사용자 계정의 AWS Kinesis Streams에 있는 스트림에 이벤트를 릴레이할 수 있도록 허용합니다.

CloudWatchEventsInvocationAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchEventsInvocationAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 14일, 18:36 UTC
- 편집된 시간: 2016년 1월 14일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchEventsReadOnlyAccess

설명: Amazon CloudWatch Events에 대한 읽기 전용 액세스를 제공합니다.

CloudWatchEventsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchEventsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 14일, 18:27 UTC
- 편집된 시간: 2022년 12월 1일, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchEventsServiceRolePolicy

설명: 경보 및 이벤트를 통해 구성된 작업을 사용자 대신 실행할 수 있습니다. AWS CloudWatch

CloudWatchEventsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 17일, 00:42 UTC
- 편집된 시간: 2017년 11월 17일, 00:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchFullAccess

설명: 에 대한 전체 액세스 권한을 제공합니다 CloudWatch.

CloudWatchFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2022년 11월 27일, 13:23 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchFullAccessV2

설명: 에 대한 전체 액세스 권한을 제공합니다 CloudWatch.

CloudWatchFullAccessV2 [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchFullAccessV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 1일, 11:32 UTC
- 편집 시간: 2024년 5월 17일 22:20 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchInternetMonitorServiceRolePolicy

설명: Internet Monitor가 사용자를 대신하여 EC2, 작업 공간, CloudFront 리소스 및 기타 필수 서비스에 액세스할 수 있도록 허용합니다.

CloudWatchInternetMonitorServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 27일, 17:46 UTC
- 편집된 시간: 2023년 7월 20일, 04:46 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchLambdaInsightsExecutionRolePolicy

설명: Lambda 인사이트 확장 프로그램에 필요한 정책

CloudWatchLambdaInsightsExecutionRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchLambdaInsightsExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 7일, 19:27 UTC
- 편집된 시간: 2020년 10월 7일, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchLogsCrossAccountSharingConfiguration

설명: Observability Access Manager 링크를 관리하고 CloudWatch 로그 리소스 공유를 설정하는 기능을 제공합니다.

CloudWatchLogsCrossAccountSharingConfiguration [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchLogsCrossAccountSharingConfiguration를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:55 UTC
- 편집된 시간: 2022년 11월 27일, 13:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchLogsFullAccess

설명: CloudWatch 로그에 대한 전체 액세스 권한을 제공합니다.

CloudWatchLogsFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchLogsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC

- 편집 시간: 2023년 11월 26일 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchLogsReadOnlyAccess

설명: CloudWatch 로그에 대한 읽기 전용 액세스를 제공합니다.

CloudWatchLogsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchLogsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 11월 26일 18:11 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchNetworkMonitorServiceRolePolicy

설명: CloudWatch Network Monitor가 사용자를 대신하여 EC2 및 VPC 리소스에 액세스 및 관리하고, 데이터를 게시하고, 다른 필수 서비스에 액세스할 수 CloudWatch 있도록 합니다.

CloudWatchNetworkMonitorServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2023년 12월 21일 18:53 UTC
- 편집 시간: 2023년 12월 21일 18:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchReadOnlyAccess

설명: 에 대한 읽기 전용 액세스를 제공합니다 CloudWatch.

CloudWatchReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 5월 17일 22:17 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchSyntheticsFullAccess

설명: CloudWatch Synthetics에 대한 전체 액세스 권한을 제공합니다.

CloudWatchSyntheticsFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchSyntheticsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 25일, 17:39 UTC
- 편집된 시간: 2022년 5월 6일, 18:14 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CloudWatchSyntheticsReadOnlyAccess

설명: CloudWatch Synthetics에 대한 읽기 전용 액세스를 제공합니다.

CloudWatchSyntheticsReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchSyntheticsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 25일, 17:45 UTC
- 편집된 시간: 2020년 3월 6일, 19:26 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "synthetics:Describe*",
      "synthetics:Get*",
      "synthetics:List*"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComprehendDataAccessRolePolicy

설명: 데이터 액세스를 위해 AWS S3 리소스에 대한 액세스를 허용하는 Comprehend 서비스 역할 정책

ComprehendDataAccessRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ComprehendDataAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 3월 6일, 22:28 UTC
- 편집된 시간: 2019년 3월 6일, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*Comprehend*",
      "arn:aws:s3::*comprehend*"
    ]
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComprehendFullAccess

설명: 아마존 Comprehend에 대한 전체 액세스 권한을 제공합니다.

ComprehendFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ComprehendFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:08 UTC
- 편집된 시간: 2017년 12월 5일, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComprehendMedicalFullAccess

설명: 아마존 Comprehend Medical에 대한 전체 액세스 권한을 제공합니다.

ComprehendMedicalFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ComprehendMedicalFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 17:55 UTC
- 편집된 시간: 2018년 11월 27일, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
{
  "Action" : [
    "comprehendmedical:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComprehendReadOnly

설명: Amazon Comprehend에 대한 읽기 전용 액세스를 제공합니다.

ComprehendReadOnly [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ComprehendReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:10 UTC
- 편집된 시간: 2022년 4월 26일, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendReadOnly

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComputeOptimizerReadOnlyAccess

설명: 에 대한 읽기 전용 액세스를 제공합니다 ComputeOptimizer.

ComputeOptimizerReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ComputeOptimizerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 3월 7일, 00:11 UTC
- 편집된 시간: 2023년 8월 28일, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ComputeOptimizerServiceRolePolicy

설명: 사용자 대신 AWS 서비스를 호출하고 워크로드 세부 정보를 수집할 수 있습니다.

ComputeOptimizer

ComputeOptimizerServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 3일, 08:45 UTC
- 편집된 시간: 2022년 6월 13일, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ConfigConformsServiceRolePolicy

설명: 적합성 AWSConfig 팩을 만드는 데 필요한 정책

ConfigConformsServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 7월 25일, 21:38 UTC
- 편집된 시간: 2023년 1월 12일, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CostOptimizationHubAdminAccess

설명: 이 관리형 정책은 관리자에게 비용 최적화 허브에 대한 액세스 권한을 제공합니다.

CostOptimizationHubAdminAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CostOptimizationHubAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 19일 00:03 UTC
- 편집 시간: 2023년 12월 19일 00:03 UTC
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CostOptimizationHubReadOnlyAccess

설명: 이 관리형 정책은 비용 최적화 허브에 대한 읽기 전용 액세스를 제공합니다.

CostOptimizationHubReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 CostOptimizationHubReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 12월 13일 18:04 UTC
- 편집 시간: 2023년 12월 13일 18:04 UTC
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```

"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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CostOptimizationHubServiceRolePolicy

설명: Cost Optimization Hub에서 조직 정보를 검색하고 최적화 관련 데이터 및 메타데이터를 수집할 수 있도록 합니다.

CostOptimizationHubServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 작성 시간: 2023년 11월 26일 08:03 UTC
- 편집 시간: 2023년 11월 26일, 08:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

CustomerProfilesServiceLinkedRolePolicy

설명: Amazon Connect 고객 프로필이 사용자를 대신하여 AWS 서비스와 리소스에 액세스할 수 있도록 허용합니다.

CustomerProfilesServiceLinkedRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 7일, 22:56 UTC
- 편집된 시간: 2023년 3월 7일, 22:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DatabaseAdministrator

설명: AWS 데이터베이스 AWS 서비스를 설정하고 구성하는 데 필요한 서비스 및 작업에 대한 전체 액세스 권한을 부여합니다.

DatabaseAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 DatabaseAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:25 UTC
- 편집된 시간: 2019년 1월 8일, 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DataScientist

설명: AWS 데이터 분석 서비스에 권한을 부여합니다.

DataScientist [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 DataScientist를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:28 UTC
- 편집된 시간: 2019년 12월 3일, 16:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DAXServiceRolePolicy

설명: 이 정책을 통해 DAX는 고객을 대신하여 네트워크 인터페이스, 보안 그룹, 서브넷 및 Vpc를 생성하고 관리할 수 있습니다.

DAXServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 5일, 17:51 UTC

- 편집된 시간: 2018년 3월 5일, 17:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

설명: Amazon DynamoDB용 Amazon CloudWatch 컨트리뷰터 인사이트를 지원하는 데 필요한 권한입니다.

DynamoDBCloudWatchContributorInsightsServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 15일, 21:13 UTC
- 편집된 시간: 2019년 11월 15일, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DynamoDBKinesisReplicationServiceRolePolicy

설명: AWS DynamoDB 액세스 권한 제공 KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 12일, 00:43 UTC
- 편집된 시간: 2020년 11월 12일, 00:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

DynamoDBReplicationServiceRolePolicy

설명: 지역 간 데이터 복제를 위해 DynamoDB에서 필요한 권한

DynamoDBReplicationServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 9일, 23:55 UTC
- 편집 시간: 2024년 1월 8일 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2FastLaunchFullAccess

설명: 이 정책은 EC2 Fast Launch 작업에 대한 전체 액세스 권한을 부여합니다.

EC2FastLaunchFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 EC2FastLaunchFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 5월 13일 22:45 UTC
- 편집 시간: 2024년 5월 13일 22:45 UTC
- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2FastLaunchServiceRolePolicy

설명: 정책에 따라 ec2fastlaunch는 고객 계정에서 사전 프로비저닝된 스냅샷을 준비 및 관리하고 관련 지표를 게시할 수 있습니다.

EC2FastLaunchServiceRolePolicy관리형 [AWS 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 1월 10일, 13:08 UTC
- 편집된 시간: 2022년 1월 10일, 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2FleetTimeShiftableServiceRolePolicy

설명: 향후에 인스턴스를 시작할 수 있는 권한을 EC2 플릿에 부여하는 정책입니다.

EC2FleetTimeShiftableServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 23일, 19:47 UTC
- 편집된 시간: 2019년 12월 23일, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
      }
    }
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Ec2ImageBuilderCrossAccountDistributionAccess

설명: EC2 Image Builder에서 계정 간 분배를 수행하는 데 필요한 권한입니다.

Ec2ImageBuilderCrossAccountDistributionAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 Ec2ImageBuilderCrossAccountDistributionAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 19:22 UTC
- 편집된 시간: 2020년 9월 30일, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/
Ec2ImageBuilderCrossAccountDistributionAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2ImageBuilderLifecycleExecutionPolicy

설명: EC2 ImageBuilderLifecycleExecutionPolicy 정책은 Image Builder에 Image Builder 이미지 리소스 및 기본 리소스 (AMI, 스냅샷) 의 사용 중단 또는 삭제와 같은 작업을 수행할 수 있는 권한을 부여하여 이미지 수명 주기 관리 작업에 대한 자동화된 규칙을 지원합니다.

EC2ImageBuilderLifecycleExecutionPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 EC2ImageBuilderLifecycleExecutionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 작성 시간: 2023년 11월 16일 23:23 UTC
- 편집 시간: 2023년 11월 16일, 23:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  },
  {
    "Sid" : "EC2DeleteSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "EC2TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*::snapshot/*",
      "arn:aws:ec2:*::image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "DeprecatedBy"
      }
    }
  },
  {
    "Sid" : "ECRIImagePermission",
    "Effect" : "Allow",
    "Action" : [
      "ecr:BatchGetImage",
      "ecr:BatchDeleteImage"
    ],
```

```

    "Resource" : "arn:aws:ecr:*:*:repository/*",
    "Condition" : {
      "StringEquals" : {
        "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "ImageBuilderEC2TagServicePermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "tag:GetResources",
      "imagebuilder:DeleteImage"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2InstanceConnect

설명: 고객이 EC2 인스턴스 연결을 호출하여 EC2 인스턴스에 임시 키를 게시하고 ssh 또는 EC2 인스턴스 연결 CLI를 통해 연결할 수 있습니다.

EC2InstanceConnect [관리형 정책입니다AWS](#).

이 정책 사용

사용자, 그룹 및 역할에 EC2InstanceConnect를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 18:53 UTC
- 편집된 시간: 2019년 6월 27일, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Ec2InstanceConnectEndpoint

설명: 고객이 생성한 EC2 인스턴스 연결 엔드포인트를 관리하기 위한 EC2 인스턴스 연결 엔드포인트 정책

Ec2InstanceConnectEndpoint [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 24일, 20:19 UTC
- 편집된 시간: 2023년 1월 24일, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
      ]
    }
  }
}
]
}
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2InstanceProfileForImageBuilder

설명: Image Builder 서비스를 위한 EC2 인스턴스 프로파일입니다.

EC2InstanceProfileForImageBuilder [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `EC2InstanceProfileForImageBuilder`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 1일, 19:08 UTC
- 편집된 시간: 2020년 8월 27일, 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

설명: EC2 Image Builder로 컨테이너 이미지를 빌드하기 위한 EC2 인스턴스 프로파일입니다. 이 정책은 사용자에게 ECR 이미지를 업로드할 수 있는 광범위한 권한을 부여합니다.

EC2InstanceProfileForImageBuilderECRContainerBuilds [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `EC2InstanceProfileForImageBuilderECRContainerBuilds`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 11일, 19:48 UTC
- 편집된 시간: 2020년 12월 11일, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ECRReplicationServiceRolePolicy

설명: ECR Replication에서 사용하거나 관리하는 리소스에 대한 액세스 AWS 서비스 및 리소스를 활성화합니다.

ECRReplicationServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 4일, 22:11 UTC
- 편집된 시간: 2020년 12월 4일, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  }
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElastiCacheServiceRolePolicy

설명: 이 정책을 사용하면 ElastiCache 캐시 관리에 필요한 AWS 리소스를 사용자 대신 관리할 수 있습니다.

ElastiCacheServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 12월 7일, 17:50 UTC
- 편집 시간: 2023년 11월 28일 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    }
  ]
}
```



```

    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElasticCacheManaged" : "true"
        }
      }
    }
  ],
  {
    "Sid" : "ModifyVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AmazonElasticCacheManaged" : "true"
      }
    }
  }
],
{
  "Sid" : "AllowAccessToElasticCacheTaggedVpcEndpoints",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElasticLoadBalancingFullAccess

설명: ElasticLoadBalancing Amazon에 대한 전체 액세스 권한과 ElasticLoadBalancing 기능 제공에 필요한 기타 서비스에 대한 제한된 액세스를 제공합니다.

ElasticLoadBalancingFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ElasticLoadBalancingFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 9월 20일, 20:42 UTC
- 편집된 시간: 2022년 11월 29일, 01:45 UTC
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

```
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElasticLoadBalancingReadOnly

설명: Amazon ElasticLoadBalancing 및 종속 서비스에 대한 읽기 전용 액세스를 제공합니다.

ElasticLoadBalancingReadOnly [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ElasticLoadBalancingReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 9월 20일, 20:17 UTC
- 편집 시간: 2023년 11월 26일 18:15 UTC
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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" : "*"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalActivationsDownloadSoftwareAccess

설명: 구매한 자산을 보고 관련 소프트웨어 및 키스타트 파일을 다운로드할 수 있는 액세스 권한

ElementalActivationsDownloadSoftwareAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ElementalActivationsDownloadSoftwareAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 8일, 17:26 UTC
- 편집된 시간: 2020년 9월 8일, 17:26 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ]
    }
  ]
}
```

```
    "elemental-activations:Download*"
  ],
  "Resource" : "*"
}
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalActivationsFullAccess

설명: Elemental 어플라이언스 및 소프트웨어로 구매한 자산을 보고 조치를 취할 수 있는 전체 권한 ElementalActivationsFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ElementalActivationsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 4일, 21:00 UTC
- 편집된 시간: 2020년 6월 4일, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalActivationsGenerateLicenses

설명: 구매한 자산을 보고 보류 중인 활성화에 대한 소프트웨어 라이선스를 생성할 수 있는 액세스
ElementalActivationsGenerateLicenses [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ElementalActivationsGenerateLicenses를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 28일, 18:28 UTC
- 편집된 시간: 2020년 8월 28일, 18:28 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalActivationsReadOnlyAccess

설명: 사용자와 관련된 구매 자산의 세부 목록에 대한 읽기 전용 액세스 AWS 계정

ElementalActivationsReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalActivationsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 28일, 16:51 UTC
- 편집된 시간: 2020년 8월 28일, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalAppliancesSoftwareFullAccess

설명: Elemental 어플라이언스 및 소프트웨어 견적 및 주문을 확인하고 조치를 취할 수 있는 전체 권한 ElementalAppliancesSoftwareFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ElementalAppliancesSoftwareFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 31일, 16:28 UTC
- 편집된 시간: 2021년 2월 5일, 21:01 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalAppliancesSoftwareReadOnlyAccess

설명: Elemental 어플라이언스 및 소프트웨어 견적 및 주문을 볼 수 있는 읽기 전용 액세스 권한

ElementalAppliancesSoftwareReadOnlyAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ElementalAppliancesSoftwareReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 1일, 22:31 UTC
- 편집된 시간: 2020년 4월 1일, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ElementalSupportCenterFullAccess

설명: Elemental 어플라이언스 및 소프트웨어 지원 사례와 제품 지원 콘텐츠를 보고 조치를 취할 수 있는 전체 권한

ElementalSupportCenterFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ElementalSupportCenterFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 25일, 18:08 UTC
- 편집된 시간: 2021년 2월 5일, 21:02 UTC

- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

EMRDescribeClusterPolicyForEMRWAL

설명: 이 정책은 Amazon EMR용 WAL 서비스가 클러스터의 상태를 찾고 반환할 수 있는 읽기 전용 권한을 부여합니다.

EMRDescribeClusterPolicyForEMRWAL [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 15일, 23:30 UTC
- 편집된 시간: 2023년 6월 15일, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

FMSServiceRolePolicy

설명: FM 서비스 연결 역할이 고객 조직 계정 내의 FM 관리 리소스에 대해 FM 관련 작업을 수행할 수 있도록 허용하는 액세스 정책입니다. AWS

FMSServiceRolePolicy [관리형 정책입니다.](#) AWS

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 28일, 23:01 UTC
- 편집 시간: 2024년 4월 22일 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

정책 버전

정책 버전: v29(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

FSxDeleteServiceLinkedRoleAccess

설명: Amazon FSx에서 Amazon S3 액세스에 대한 서비스 연결 역할을 삭제할 수 있도록 허용합니다.

FSxDeleteServiceLinkedRoleAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 28일, 10:40 UTC
- 편집된 시간: 2018년 11월 28일, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
}
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GameLiftGameServerGroupPolicy

설명: GameServerGroups Gamelift가 고객 리소스를 관리할 수 있도록 허용하는 정책

GameLiftGameServerGroupPolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 GameLiftGameServerGroupPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 3일, 23:12 UTC
- 편집된 시간: 2020년 5월 13일, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:aws:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:aws:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GlobalAcceleratorFullAccess

설명: GlobalAccelerator 사용자에게 모든 API에 대한 전체 액세스 허용

GlobalAcceleratorFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 GlobalAcceleratorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 02:44 UTC
- 편집된 시간: 2020년 12월 4일, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GlobalAcceleratorReadOnlyAccess

설명: GlobalAccelerator 사용자에게 읽기 전용 API 액세스 허용

GlobalAcceleratorReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 GlobalAcceleratorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 02:41 UTC
- 편집된 시간: 2018년 11월 27일, 02:41 UTC

- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GreengrassOTAUpdateArtifactAccess

설명: 모든 그린그래스 지역의 Greengrass OTA 업데이트 아티팩트에 대한 읽기 액세스 권한을 제공합니다.

GreengrassOTAUpdateArtifactAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 GreengrassOTAUpdateArtifactAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 29일, 18:11 UTC
- 편집된 시간: 2018년 12월 18일, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```


자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GroundTruthSyntheticConsoleFullAccess

설명: 이 정책은 SageMaker Ground Truth Synthetic 콘솔의 모든 기능을 사용하는 데 필요한 권한을 부여합니다.

GroundTruthSyntheticConsoleFullAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 GroundTruthSyntheticConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 25일, 15:58 UTC
- 편집된 시간: 2022년 8월 25일, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker-groundtruth-synthetic:*",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

GroundTruthSyntheticConsoleReadOnlyAccess

설명: 이 정책은 를 통해 SageMaker Ground Truth Synthical에 대한 읽기 전용 액세스 권한을 부여합니다 AWS Management Console.

GroundTruthSyntheticConsoleReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 GroundTruthSyntheticConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 25일, 15:58 UTC
- 편집된 시간: 2022년 8월 25일, 15:58 UTC

- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Health_OrganizationsServiceRolePolicy

설명: 조직 보기 기능을 활성화하기 위한 AWS 건강 정책

Health_OrganizationsServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 16일, 13:28 UTC
- 편집 시간: 2024년 2월 6일 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMAccessAdvisorReadOnly

설명: 이 정책은 IAM 액세스 어드바이저가 제공하는 모든 액세스 정보 (예: 서비스에서 마지막으로 액세스한 정보) 를 읽을 수 있는 액세스 권한을 부여합니다.

IAMAccessAdvisorReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMAccessAdvisorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 21일, 19:33 UTC
- 편집된 시간: 2019년 6월 21일, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMAccessAnalyzerFullAccess

설명: IAM 액세스 분석기에 대한 전체 액세스 권한을 제공합니다.

IAMAccessAnalyzerFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMAccessAnalyzerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 2일, 17:12 UTC
- 편집된 시간: 2019년 12월 2일, 17:12 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMAccessAnalyzerReadOnlyAccess

설명: IAM 액세스 분석기 리소스에 대한 읽기 전용 액세스를 제공합니다.

IAMAccessAnalyzerReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMAccessAnalyzerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 2일, 17:12 UTC
- 편집 시간: 2023년 11월 27일 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMFullAccess

설명: 를 통해 IAM에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

IAMFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 6월 21일, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMReadOnlyAccess

설명: 를 통해 IAM에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

IAMReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2018년 1월 25일, 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMSelfManageServiceSpecificCredentials

설명: IAM 사용자가 자신의 서비스별 자격 증명을 관리할 수 있도록 허용합니다.

IAMSelfManageServiceSpecificCredentials [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMSelfManageServiceSpecificCredentials를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 22일, 17:25 UTC
- 편집된 시간: 2016년 12월 22일, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMUserChangePassword

설명: IAM 사용자가 자신의 비밀번호를 변경할 수 있는 기능을 제공합니다.

IAMUserChangePassword [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMUserChangePassword를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 15일, 00:25 UTC
- 편집된 시간: 2016년 11월 15일, 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IAMUserSSHKeys

설명: IAM 사용자가 자신의 SSH 키를 관리할 수 있는 기능을 제공합니다.

IAMUserSSHKeys [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMUserSSHKeys를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:08 UTC
- 편집된 시간: 2015년 7월 9일, 17:08 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IVSFullAccess

설명: 대화형 비디오 서비스 (IVS) 에 대한 전체 액세스 권한을 제공하며 ivs 콘솔에 완전히 액세스하는데 필요한 종속 서비스에 대한 권한도 포함됩니다.

IVSFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 IVSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 13일 21:20 UTC
- 편집 시간: 2023년 12월 13일 21:20 UTC
- ARN: arn:aws:iam::aws:policy/IVSFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
```

```
    "Action" : [
      "ivs:*",
      "ivschat:*"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IVSReadOnlyAccess

설명: IVS 저지연 및 실시간 스트리밍 API에 대한 읽기 전용 액세스를 제공합니다.

IVSReadOnlyAccess [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 IVSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 5일 18:00 UTC
- 편집 시간: 2024년 2월 16일 18:03 UTC
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

IVSRecordToS3

설명: S3를 수행하여 IVS 라이브 PutObject 스트림을 녹화하는 서비스 연결 역할

IVSRecordToS3 [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 5일, 00:10 UTC
- 편집된 시간: 2020년 12월 5일, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

KafkaConnectServiceRolePolicy

설명: 이 정책은 Kafka Connect에 사용자 대신 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

KafkaConnectServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 7일, 13:12 UTC
- 편집된 시간: 2021년 9월 7일, 13:12 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

KafkaServiceRolePolicy

설명: Kafka용 IAM 서비스 연결 역할 정책입니다.

KafkaServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 15일, 23:31 UTC
- 편집된 시간: 2023년 4월 28일, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
    }
  }
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

KeyspacesReplicationServiceRolePolicy

설명: 지역 간 데이터 복제를 위해 Keyspace에서 요구하는 권한

KeyspacesReplicationServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 2일, 16:15 UTC
- 편집된 시간: 2023년 5월 2일, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cassandra:Select",
      "cassandra:SelectMultiRegionResource",
      "cassandra:Modify",
      "cassandra:ModifyMultiRegionResource"
    ],
    "Resource" : "*"
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

LakeFormationDataAccessServiceRolePolicy

설명: Lake Formation 리소스에 대한 임시 데이터 액세스 권한을 부여하는 정책

LakeFormationDataAccessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 20일, 20:46 UTC
- 편집 시간: 2024년 2월 6일 18:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

LexBotPolicy

설명: AWS Lex Bot 사용 사례에 대한 정책

LexBotPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 2월 17일, 22:18 UTC
- 편집된 시간: 2019년 11월 13일, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
```

```
    "Resource" : [
      "*"
    ]
  }
]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

LexChannelPolicy

설명: AWS Lex 채널 사용 사례에 대한 정책

LexChannelPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 2월 17일, 23:23 UTC
- 편집된 시간: 2017년 2월 17일, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

LightsailExportAccess

설명: AWS 리소스를 내보낼 권한을 부여하는 Lightsail 서비스 연결 역할 정책

LightsailExportAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 9월 28일, 16:35 UTC
- 편집된 시간: 2022년 1월 15일, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```


자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MediaConnectGatewayInstanceRolePolicy

설명: 이 정책은 MediaConnect 게이트웨이 인스턴스를 게이트웨이에 등록할 권한을 부여합니다.
MediaConnect

MediaConnectGatewayInstanceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 MediaConnectGatewayInstanceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 22일, 20:43 UTC
- 편집된 시간: 2023년 3월 22일, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```

    "Sid" : "MediaConnectGateway",
    "Effect" : "Allow",
    "Action" : [
        "mediacconnect:DiscoverGatewayPollEndpoint",
        "mediacconnect:PollGateway",
        "mediacconnect:SubmitGatewayStateChange"
    ],
    "Resource" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MediaPackageServiceRolePolicy

설명: 에 로그를 MediaPackage 게시할 수 있습니다. CloudWatch

MediaPackageServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 9월 18일, 17:45 UTC
- 편집된 시간: 2020년 9월 18일, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MemoryDBServiceRolePolicy

설명: 이 정책은 MemoryDB가 리소스 관리에 필요한 경우 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

MemoryDBServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 17일, 22:34 UTC
- 편집된 시간: 2021년 8월 18일, 23:48UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MigrationHubDMSAccessServiceRolePolicy

설명: Database Migration Service가 고객 계정에서 역할을 맡아 Migration Hub에 전화를 걸도록 하는 정책

MigrationHubDMSAccessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 17:50 UTC

- 편집된 시간: 2019년 10월 7일, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MigrationHubServiceRolePolicy

설명: Migration Hub에서 사용자를 대신하여 Application Discovery Service를 호출할 수 있도록 합니다.

MigrationHubServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 17:22 UTC
- 편집된 시간: 2020년 8월 6일, 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
      "*"
    ]
  }
]
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MigrationHubSMSAccessServiceRolePolicy

설명: 서버 마이그레이션 서비스가 고객 계정에서 Migration Hub를 호출하는 역할을 담당하도록 하는 정책

MigrationHubSMSAccessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 18:30 UTC
- 편집된 시간: 2019년 10월 7일, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

MonitronServiceRolePolicy

설명: 필수 고객 리소스에 대한 액세스 권한을 부여하는 AWS Monitron 서비스 연결 역할에 대한 정책입니다.

MonitronServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 5월 2일, 19:22 UTC
- 편집된 시간: 2022년 5월 2일, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

NeptuneConsoleFullAccess

설명: 를 사용하여 Amazon Neptune을 관리할 수 있는 전체 액세스 권한을 제공합니다. AWS Management Console참고로 이 정책은 또한 계정 내의 모든 SNS 주제에 대해 게시할 수 있는 전체 액세스, Amazon EC2 인스턴스 및 VPC 구성을 생성 및 편집할 수 있는 권한, Amazon KMS에서 키를 보고 나열할 수 있는 권한, Amazon RDS에 대한 전체 액세스도 부여합니다. 자세한 내용은 <https://aws.amazon.com/neptune/faqs/>를 참조하세요.

NeptuneConsoleFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 19일, 21:35 UTC
- 편집 시간: 2023년 11월 30일 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneConsoleFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

NeptuneFullAccess

설명: Amazon Neptune에 대한 전체 액세스 권한을 제공합니다. 참고로 이 정책은 계정 내 모든 SNS 주제에 대한 게시에 대한 전체 액세스와 Amazon RDS에 대한 전체 액세스도 부여합니다. 자세한 내용은 <https://aws.amazon.com/neptune/faqs/>를 참조하세요.

NeptuneFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 30일, 19:17 UTC
- 편집 시간: 2024년 1월 22일 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
      "*"
    ]
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

NeptuneGraphReadOnlyAccess

설명: 종속 서비스에 대한 읽기 전용 권한과 함께 모든 Amazon Neptune 분석 리소스에 대한 읽기 전용 액세스를 제공합니다.

NeptuneGraphReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneGraphReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 30일 07:32 UTC
- 편집 시간: 2023년 11월 30일, 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

NeptuneReadOnlyAccess

설명: Amazon Neptune에 대한 읽기 전용 액세스를 제공합니다. 참고로 이 정책은 Amazon RDS 리소스에 대한 액세스 권한도 부여합니다. 자세한 내용은 <https://aws.amazon.com/neptune/faqs/>를 참조하세요.

NeptuneReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 30일, 19:16 UTC
- 편집 시간: 2024년 1월 22일 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
"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" : [
    "*"
  ]
}
```

```
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

NetworkAdministrator

설명: AWS 네트워크 리소스를 설정하고 구성하는 데 필요한 AWS 서비스 및 작업에 대한 전체 액세스 권한을 부여합니다.

NetworkAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 NetworkAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:31 UTC
- 편집된 시간: 2021년 9월 16일, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

OAMFullAccess

설명: CloudWatch 오픈서버빌리티 액세스 관리자에 대한 전체 액세스 권한을 제공합니다.

OAMFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 OAMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:38 UTC
- 편집된 시간: 2022년 11월 27일, 13:38 UTC
- ARN: arn:aws:iam::aws:policy/OAMFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

OAMReadOnlyAccess

설명: CloudWatch 오픈서버빌리티 액세스 관리자에 대한 읽기 전용 액세스를 제공합니다.

OAMReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 OAMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:29 UTC
- 편집된 시간: 2022년 11월 27일, 13:29 UTC
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

OpensearchIngestionSelfManagedVpcePolicy

설명: Amazon OpenSearch Ingestion에서 네트워크 리소스를 설명하고 클라우드 위치에 서비스 지표를 작성할 수 있도록 허용합니다.

OpensearchIngestionSelfManagedVpcePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 6월 10일 19:59 UTC
- 편집 시간: 2024년 6월 10일 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

PartnerCentralAccountManagementUserRoleAssociation

설명: 파트너 중앙 사용자를 IAM 역할과 연결 및 분리할 수 있는 액세스 권한을 제공합니다.

PartnerCentralAccountManagementUserRoleAssociation [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 PartnerCentralAccountManagementUserRoleAssociation를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 10일, 02:03 UTC
- 편집된 시간: 2023년 11월 10일, 02:03 UTC
- ARN: arn:aws:iam::aws:policy/
PartnerCentralAccountManagementUserRoleAssociation

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

PowerUserAccess

설명: AWS 서비스 및 리소스에 대한 전체 액세스 권한을 제공하지만 사용자 및 그룹 관리는 허용하지 않습니다.

PowerUserAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 PowerUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2023년 7월 6일, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

QBusinessServiceRolePolicy

설명: Amazon Q에서 사용하거나 관리하는 AWS 서비스 권한과 리소스를 부여합니다.

QBusinessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 4월 29일 16:05 UTC
- 편집 시간: 2024년 4월 29일 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
      }
    }
  }
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

설명: QuickSight 팀에서 S3 스토리지 관리 분석에서 생성한 고객 데이터에 액세스하는 데 사용하는 정책입니다.

QuickSightAccessForS3StorageManagementAnalyticsReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 QuickSightAccessForS3StorageManagementAnalyticsReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 6월 12일, 18:18 UTC
- 편집된 시간: 2019년 10월 8일, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

RDSCloudHsmAuthorizationRole

설명: Amazon RDS 서비스 역할에 대한 기본 정책입니다.

RDSCloudHsmAuthorizationRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 RDSCloudHsmAuthorizationRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2019년 9월 26일, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ReadOnlyAccess

설명: AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다.

ReadOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 5월 16일 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

정책 버전

정책 버전: v113(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:ListTrustedIdentityPropagationsForConsole",
"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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ResourceGroupsandTagEditorFullAccess

설명: Resource Groups 및 태그 편집기에 대한 전체 액세스 권한을 제공합니다.

ResourceGroupsandTagEditorFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ResourceGroupsandTagEditorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC

- 편집된 시간: 2023년 8월 10일, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)

- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ResourceGroupsandTagEditorReadOnlyAccess

설명: Resource Groups 및 Tag Editor를 사용할 수 있는 액세스를 제공하지만 태그 편집기를 통한 태그 편집은 허용하지 않습니다.

ResourceGroupsandTagEditorReadOnlyAccess [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ResourceGroupsandTagEditorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2023년 8월 10일, 13:42 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ResourceGroupsServiceRolePolicy

설명: AWS Resource Groups가 리소스를 소유한 AWS 서비스를 쿼리하여 그룹을 유지할 수 있도록 합니다. up-to-date

ResourceGroupsServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 5일, 16:57 UTC
- 편집된 시간: 2023년 1월 5일, 16:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

설명: OpenShift Amazon EBS 컨테이너 스토리지 인터페이스 (CSI) 드라이버 운영자가 ROSA AWS (Red Hat OpenShift 서비스 온) 클러스터에 Amazon EBS CSI 드라이버를 설치하고 유지 관리할 수 있도록 허용합니다. Amazon EBS CSI 드라이버를 사용하면 ROSA 클러스터가 영구 볼륨에 대한 Amazon EBS 볼륨의 수명 주기를 관리할 수 있습니다.

R0SAAmazonEBSCSIDriverOperatorPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 R0SAAmazonEBSCSIDriverOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:36 UTC
- 편집된 시간: 2023년 4월 20일, 22:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/R0SAAmazonEBSCSIDriverOperatorPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSACloudNetworkConfigOperatorPolicy

설명: OpenShift 클라우드 네트워크 구성 컨트롤러 운영자가 OpenShift ROSA AWS (ROSA) 클러스터 네트워킹 오버레이에서 사용할 네트워킹 리소스를 프로비저닝하고 관리할 수 있도록 합니다. OpenShift 클라우드 네트워크 운영자는 를 통해 네트워크 플러그인을 대신하여 AWS API와 인터페이스합니다. CustomResourceDefinitions 운영자는 이러한 정책 권한을 사용하여 ROSA 클러스터의 일부인 Amazon EC2 인스턴스의 프라이빗 IP 주소를 관리합니다.

ROSACloudNetworkConfigOperatorPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSACloudNetworkConfigOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:34 UTC
- 편집된 시간: 2023년 4월 20일, 22:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAControlPlaneOperatorPolicy

설명: OpenShift ROSA AWS (ROSA) 컨트롤 플레인에서 ROSA 클러스터 아마존 EC2 및 아마존 Route 53 리소스를 관리할 수 있도록 합니다.

ROSAControlPlaneOperatorPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAControlPlaneOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 24일, 23:02 UTC
- 편집된 시간: 2023년 6월 30일, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAImageRegistryOperatorPolicy

설명: OpenShift 이미지 레지스트리 운영자가 ROSA AWS (Red Hat OpenShift Service on) 클러스터 내 이미지 레지스트리에서 사용할 Amazon S3 버킷과 객체를 프로비저닝하고 관리하여 ROSA 스토리지 요구 사항을 충족할 수 있도록 합니다. OpenShift 이미지 레지스트리 운영자는 Red Hat 클러스터의 내부 레지스트리를 설치하고 유지 관리합니다. OpenShift

ROSAImageRegistryOperatorPolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAImageRegistryOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:13 UTC
- 편집 시간: 2023년 12월 12일 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}/*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAIngressOperatorPolicy

설명: OpenShift 인그레스 오퍼레이터가 ROSA (Red Hat OpenShift Service on AWS) 클러스터의 로드 밸런서 및 도메인 이름 시스템 (DNS) 구성을 프로비저닝하고 관리할 수 있도록 합니다. 이 정책은 운영자가 호스팅 영역을 검색하기 위해 Route 53 리소스를 필터링하는 태그 값에 대한 읽기 액세스를 허용합니다.

ROSAIngressOperatorPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAIngressOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:37 UTC
- 편집된 시간: 2023년 4월 20일, 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAInstallerPolicy

설명: ROSA AWS (Red Hat OpenShift Service on) 설치 프로그램이 ROSA 클러스터 설치를 지원하는 AWS 리소스를 관리할 수 있도록 허용합니다. 여기에는 ROSA 워커 노드에 대한 인스턴스 프로파일 관리가 포함됩니다.

ROSAInstallerPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAInstallerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 6일, 21:00 UTC
- 편집 시간: 2024년 4월 24일 19:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAKMSProviderPolicy

설명: 내장된 ROSA AWS 암호화 공급자가 KMS (AWS 키 관리 서비스) 키를 관리하여 고객이 제공한 AWS KMS 키를 사용하여 etcd 데이터 암호화를 지원할 수 있습니다. 이 정책은 KMS 키를 사용한 데이터 암호화 및 암호 해독을 허용합니다.

ROSAKMSProviderPolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAKMSProviderPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:10 UTC
- 편집된 시간: 2023년 4월 27일, 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAKubeControllerPolicy

설명: ROSA 쿠버네티스 컨트롤러가 ROSA 클러스터의 Amazon EC2, Elastic Load Balancing (ELB) AWS 및 KMS (키 관리 서비스) 리소스를 관리할 수 있도록 합니다.

ROSAKubeControllerPolicy [관리형 정책입니다AWS](#).

이 정책 사용

사용자, 그룹 및 역할에 ROSAKubeControllerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:09 UTC
- 편집된 시간: 2023년 10월 16일, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAManageSubscription

설명: 이 정책은 OpenShift ROSA AWS (ROSA) 서브스크립션을 관리하는 데 필요한 권한을 제공합니다.

ROSAManageSubscription [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAManageSubscription를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 11일, 20:58 UTC
- 편집된 시간: 2023년 8월 4일, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{  
  "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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSANodePoolManagementPolicy

설명: Red Hat OpenShift Service on AWS (ROSA) 이 보안 그룹을 구성하고 인스턴스 및 볼륨에 태그를 지정할 수 있는 권한을 포함하여 클러스터 EC2 인스턴스를 작업자 노드로 관리할 수 있도록 허용합니다. 또한 이 정책은 KMS (AWS 키 관리 서비스) 키로 제공되는 디스크 암호화와 함께 EC2 인스턴스를 사용할 수 있도록 허용합니다.

ROSANodePoolManagementPolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSANodePoolManagementPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 8일, 20:48 UTC
- 편집 시간: 2024년 5월 2일 14:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  }
}
```

```
    }  
  }  
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSASRESupportPolicy

설명: ROSA 클러스터 노드 상태를 변경하는 기능을 포함하여 ROSA (ROSA) 클러스터에서 Red Hat OpenShift Service와 관련된 AWS 리소스를 초기에 관찰, 진단 및 지원하는 데 필요한 권한을 ROSA 사이트 신뢰성 엔지니어링 AWS (SRE) 에 제공합니다.

ROSASRESupportPolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSASRESupportPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 1일, 14:36 UTC
- 편집 시간: 2024년 4월 10일 20:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ROSAWorkerInstancePolicy

설명: 사용자 계정의 ROSA AWS (ROSA) 워커 노드에서 Amazon EC2 인스턴스에 대한 읽기 전용 액세스 AWS 리전 및 컴퓨팅 노드 수명 주기 관리를 위한 Red Hat OpenShift Service를 허용합니다.

ROSAWorkerInstancePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ROSAWorkerInstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:35 UTC
- 편집된 시간: 2023년 4월 20일, 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Route53RecoveryReadinessServiceRolePolicy

설명: Route 53 복구 준비를 위한 서비스 연결 역할 정책

Route53RecoveryReadinessServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 7월 15일, 16:06 UTC
- 편집된 시간: 2023년 2월 14일, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

Route53ResolverServiceRolePolicy

설명: Route53 리졸버에서 사용하거나 관리하는 리소스에 대한 액세스 AWS 서비스 및 리소스를 활성화합니다.

Route53ResolverServiceRolePolicy [관리형 정책입니다.AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 12일, 17:47 UTC

- 편집된 시간: 2020년 8월 12일, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

S3StorageLensServiceRolePolicy

설명: S3 Storage Lens에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다.

S3StorageLensServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 18일, 18:15 UTC
- 편집된 시간: 2020년 11월 18일, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```

    "organizations:ListAccounts",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SecretsManagerReadWrite

설명: 를 통해 AWS Secrets Manager에 대한 읽기/쓰기 액세스 권한을 제공합니다. AWS Management Console참고: 여기에는 IAM 작업이 제외되므로 순환 구성이 필요한 경우 IAM과 함께 사용하십시오 FullAccess .

SecretsManagerReadWrite [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 SecretsManagerReadWrite를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 4일, 18:05 UTC
- 편집 시간: 2024년 2월 22일 18:12 UTC
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*/*"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SecurityAudit

설명: 보안 감사 템플릿은 보안 구성 메타데이터를 읽을 수 있는 액세스 권한을 부여합니다. AWS 계정의 구성을 감사하는 소프트웨어에 유용합니다.

SecurityAudit [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 SecurityAudit를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 4월 5일 17:32 UTC
- ARN: arn:aws:iam::aws:policy/SecurityAudit

정책 버전

정책 버전: v42(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
  ]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SecurityLakeServiceLinkedRole

설명: 이 정책은 사용자를 대신하여 Amazon Security Lake 서비스를 운영할 수 있는 권한을 부여합니다.

SecurityLakeServiceLinkedRole [AWS 관리형 정책입니다](#).

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 29일, 14:03 UTC
- 편집 시간: 2024년 4월 19일 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        ]
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServerMigration_ServiceRole

설명: AWS 서버 마이그레이션 서비스가 VM을 EC2로 마이그레이션할 수 있는 권한: 서버 마이그레이션 서비스가 마이그레이션된 리소스를 고객의 EC2 계정에 배치할 수 있도록 허용합니다.

ServerMigration_ServiceRole [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 ServerMigration_ServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2020년 8월 11일, 20:41 UTC
- 편집된 시간: 2020년 10월 15일, 17:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*/*"
    }
  }
}
]

```

}

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServerMigrationConnector

설명: AWS 서버 마이그레이션 커넥터가 VM을 EC2로 마이그레이션할 수 있도록 허용하는 권한. AWS 서버 마이그레이션 서비스와의 통신, 'sms-b-' 및 import-to-ec '2-'로 시작하는 S3 버킷, 서버 마이그레이션 커넥터 업그레이드, AWS 서버 마이그레이션 커넥터 등록 및 메트릭 업로드에 사용되는 버킷에 대한 읽기/쓰기 액세스를 허용합니다. AWS

ServerMigrationConnector [관리형 정책입니다.](#) AWS

이 정책 사용

사용자, 그룹 및 역할에 ServerMigrationConnector를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 10월 24일, 21:45 UTC
- 편집된 시간: 2016년 10월 24일, 21:45 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationConnector

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServerMigrationServiceConsoleFullAccess

설명: 서버 마이그레이션 서비스 콘솔의 모든 기능을 사용하는 데 필요한 권한

ServerMigrationServiceConsoleFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServerMigrationServiceConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2020년 5월 9일, 17:18 UTC
- 편집된 시간: 2020년 7월 20일, 22:00 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServerMigrationServiceLaunchRole

설명: AWS 서버 마이그레이션 서비스가 마이그레이션된 서버 및 애플리케이션을 시작하는 데 AWS 필요한 관련 리소스를 만들고 고객의 AWS 계정 리소스에 업데이트할 수 있는 권한입니다.

ServerMigrationServiceLaunchRole [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServerMigrationServiceLaunchRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 26일, 19:53 UTC
- 편집된 시간: 2020년 10월 15일, 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      }
    }
  }
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServerMigrationServiceRoleForInstanceValidation

설명: AWS SMS가 사용된 데이터 검증 스크립트를 실행하고 스크립트 성공/실패를 SMS로 다시 보낼 수 있도록 허용하는 권한

ServerMigrationServiceRoleForInstanceValidation [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServerMigrationServiceRoleForInstanceValidation를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 7월 20일, 22:25 UTC
- 편집된 시간: 2020년 7월 20일, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServiceQuotasFullAccess

설명: Service Quotas에 대한 전체 액세스 권한 제공

ServiceQuotasFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServiceQuotasFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 24일, 15:44 UTC
- 편집된 시간: 2021년 2월 4일, 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServiceQuotasReadOnlyAccess

설명: Service Quotas에 대한 읽기 전용 액세스를 제공합니다.

ServiceQuotasReadOnlyAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServiceQuotasReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 24일, 15:31 UTC
- 편집된 시간: 2020년 12월 21일, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ServiceQuotasServiceRolePolicy

설명: Service Quotas가 사용자를 대신하여 지원 사례를 생성할 수 있습니다.

ServiceQuotasServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 5월 22일, 20:44 UTC
- 편집된 시간: 2019년 6월 24일, 14:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SimpleWorkflowFullAccess

설명: 단순 워크플로우 구성 서비스에 대한 전체 액세스 권한을 제공합니다.

SimpleWorkflowFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 SimpleWorkflowFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SplitCostAllocationDataServiceRolePolicy

설명: 분할 비용 할당 데이터를 사용하여 해당하는 경우 AWS Organizations 정보를 검색하고 고객이 선택한 분할 비용 할당 데이터 서비스에 대한 원격 분석 데이터를 수집할 수 있습니다.

SplitCostAllocationDataServiceRolePolicy [AWS 관리형 정책](#)입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 4월 16일 16:05 UTC
- 편집 시간: 2024년 4월 16일 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SupportUser

설명: 이 정책은 에서 문제를 해결하고 해결할 수 있는 AWS 계정권한을 부여합니다. 또한 이 정책을 통해 사용자는 AWS 지원팀에 문의하여 사례를 생성하고 관리할 수 있습니다.

SupportUser [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 SupportUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:21 UTC
- 편집된 시간: 2023년 8월 25일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

SystemAdministrator

설명: 애플리케이션 및 개발 작업에 필요한 리소스에 필요한 전체 액세스 권한을 부여합니다.

SystemAdministrator [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 SystemAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:23 UTC
- 편집된 시간: 2020년 8월 24일, 20:05 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:ReportInstanceState",
"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"
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

TranslateFullAccess

설명: Amazon Translate에 대한 전체 액세스 권한을 제공합니다.

TranslateFullAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 TranslateFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 23:36 UTC
- 편집된 시간: 2020년 1월 8일, 21:22 UTC
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

TranslateReadOnly

설명: Amazon Translate에 대한 읽기 전용 액세스를 제공합니다.

TranslateReadOnly [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 TranslateReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:22 UTC
- 편집된 시간: 2023년 5월 24일, 17:19 UTC
- ARN: arn:aws:iam::aws:policy/TranslateReadOnly

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

ViewOnlyAccess

설명: 이 정책은 모든 AWS 서비스의 리소스 및 기본 메타데이터를 볼 수 있는 권한을 부여합니다.

ViewOnlyAccess [AWS 관리형 정책](#)입니다.

이 정책 사용

사용자, 그룹 및 역할에 ViewOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:20 UTC
- 편집 시간: 2024년 6월 10일 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

정책 버전

정책 버전: v19(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*",
```

```
"mediacconnect:ListEntitlements",
"mediacconnect:ListFlows",
"mediacconnect:ListOfferings",
"mediacconnect: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"
]
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

VMImportExportRoleForAWSConnector

설명: Connector를 사용하는 고객을 위한 VM 가져오기/내보내기 서비스 역할에 대한 기본 정책입니다. AWS VM Import/Export 서비스는 이 정책에 따라 AWS Connector 가상 어플라이언스의 가상 시스템 마이그레이션 요청을 수행하는 역할을 맡습니다. (참고로 AWS Connector는 "AWSConnector" 관리형 정책을 사용하여 고객을 대신하여 VM Import/Export 서비스에 요청을 보냅니다.) AMI 및 EBS 스냅샷을 생성하고, EBS 스냅샷 속성을 수정하고, EC2 객체에 대해 "Describe*"를 호출하고, '2-'로 시작하는 S3 버킷에서 읽을 수 있는 기능을 제공합니다. import-to-ec

VMImportExportRoleForAWSConnector [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 VMImportExportRoleForAWSConnector를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 9월 3일, 20:48 UTC
- 편집된 시간: 2015년 9월 3일, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

VPCLatticeFullAccess

설명: Amazon VPC Lattice에 대한 전체 액세스 권한과 종속성 서비스에 대한 액세스를 제공합니다.

VPCLatticeFullAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 VPCLatticeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:49 UTC
- 편집된 시간: 2023년 3월 30일, 02:49 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
]
}

```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

VPCLatticeReadOnlyAccess

설명: 를 통해 Amazon VPC Lattice에 대한 읽기 전용 액세스를 제공하고 AWS Management Console 종속성 서비스에 대한 제한된 액세스를 제공합니다.

VPCLatticeReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 VPCLatticeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:47 UTC
- 편집된 시간: 2023년 3월 30일, 02:47 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
}
]
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

VPCLatticeServicesInvokeAccess

설명: Amazon VPC Lattice 서비스 호출에 대한 액세스를 제공합니다.

VPCLatticeServicesInvokeAccess [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 VPCLatticeServicesInvokeAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:45 UTC
- 편집된 시간: 2023년 3월 30일, 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WAFLoggingServiceRolePolicy

설명: 고객 로그를 Firehose 스트림에 기록하기 위한 SLR 생성

WAFLoggingServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 24일, 21:05 UTC
- 편집된 시간: 2018년 8월 24일, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WAFRegionalLoggingServiceRolePolicy

설명: 고객 로그를 Firehose 스트림에 기록하기 위한 SLR 생성

WAFRegionalLoggingServiceRolePolicy [AWS 관리형](#) 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 24일, 18:40 UTC
- 편집된 시간: 2018년 8월 24일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
```

```
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"  
    ]  
}  
]  
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WAFV2LoggingServiceRolePolicy

설명: 이 정책은 AWS WAF가 Amazon Kinesis Data Firehose에 로그를 쓸 수 있도록 하는 서비스 연결 역할을 생성합니다.

WAFV2LoggingServiceRolePolicy [관리형 정책입니다.](#) [AWS](#)

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 7일, 00:40 UTC
- 편집 시간: 2024년 6월 3일 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WellArchitectedConsoleFullAccess

설명: AWS Well-Architected 도구에 대한 전체 액세스 권한을 제공합니다. AWS Management Console

WellArchitectedConsoleFullAccess [AWS 관리형](#) 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 WellArchitectedConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 18:19 UTC
- 편집된 시간: 2018년 11월 29일, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WellArchitectedConsoleReadOnlyAccess

설명: AWS Well-Architected Tool에 대한 읽기 전용 액세스를 제공합니다. AWS Management Console

WellArchitectedConsoleReadOnlyAccess [관리형 정책입니다.AWS](#)

이 정책 사용

사용자, 그룹 및 역할에 WellArchitectedConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 18:21 UTC
- 편집된 시간: 2023년 6월 29일, 17:16 UTC
- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

WorkLinkServiceRolePolicy

설명: Amazon에서 사용하거나 관리하는 리소스에 AWS 서비스 액세스하고 리소스를 관리할 수 있습니다. WorkLink

WorkLinkServiceRolePolicy [AWS 관리형 정책입니다.](#)

이 정책 사용

사용자, 그룹 및 역할에 WorkLinkServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 23일, 19:03 UTC
- 편집된 시간: 2019년 1월 23일, 19:03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- [IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.](#)
- [IAM 자격 증명 권한 추가 및 제거](#)
- [IAM 정책의 버전 관리 이해](#)
- [AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.](#)

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.