



Reference Guide

AWS Managed Policy



AWS Managed Policy: Reference Guide

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What are AWS managed policies?	1
Understanding policy reference pages	1
Deprecated AWS managed policies	2
AWS managed policies	3
AccessAnalyzerServiceRolePolicy	44
Using this policy	44
Policy details	44
Policy version	44
JSON policy document	45
Learn more	47
AdministratorAccess	47
Using this policy	47
Policy details	47
Policy version	48
JSON policy document	48
Learn more	48
AdministratorAccess-Amplify	48
Using this policy	48
Policy details	49
Policy version	49
JSON policy document	49
Learn more	59
AdministratorAccess-AWSElasticBeanstalk	60
Using this policy	60
Policy details	60
Policy version	60
JSON policy document	60
Learn more	68
AlexaForBusinessDeviceSetup	69
Using this policy	69
Policy details	69
Policy version	69
JSON policy document	69
Learn more	70

AlexaForBusinessFullAccess	70
Using this policy	70
Policy details	70
Policy version	71
JSON policy document	71
Learn more	72
AlexaForBusinessGatewayExecution	72
Using this policy	73
Policy details	73
Policy version	73
JSON policy document	73
Learn more	74
AlexaForBusinessLifesizeDelegatedAccessPolicy	74
Using this policy	74
Policy details	74
Policy version	75
JSON policy document	75
Learn more	77
AlexaForBusinessNetworkProfileServicePolicy	77
Using this policy	77
Policy details	78
Policy version	78
JSON policy document	78
Learn more	79
AlexaForBusinessPolyDelegatedAccessPolicy	79
Using this policy	79
Policy details	79
Policy version	79
JSON policy document	80
Learn more	81
AlexaForBusinessReadOnlyAccess	82
Using this policy	82
Policy details	82
Policy version	82
JSON policy document	82
Learn more	83

AmazonAPIGatewayAdministrator	83
Using this policy	83
Policy details	83
Policy version	83
JSON policy document	84
Learn more	84
AmazonAPIGatewayInvokeFullAccess	84
Using this policy	84
Policy details	84
Policy version	85
JSON policy document	85
Learn more	85
AmazonAPIGatewayPushToCloudWatchLogs	85
Using this policy	86
Policy details	86
Policy version	86
JSON policy document	86
Learn more	87
AmazonAppFlowFullAccess	87
Using this policy	87
Policy details	87
Policy version	87
JSON policy document	88
Learn more	90
AmazonAppFlowReadOnlyAccess	91
Using this policy	91
Policy details	91
Policy version	91
JSON policy document	91
Learn more	92
AmazonAppStreamFullAccess	92
Using this policy	92
Policy details	92
Policy version	92
JSON policy document	93
Learn more	94

AmazonAppStreamPCAAccess	95
Using this policy	95
Policy details	95
Policy version	95
JSON policy document	95
Learn more	96
AmazonAppStreamReadOnlyAccess	96
Using this policy	96
Policy details	96
Policy version	97
JSON policy document	97
Learn more	97
AmazonAppStreamServiceAccess	97
Using this policy	98
Policy details	98
Policy version	98
JSON policy document	98
Learn more	99
AmazonAthenaFullAccess	99
Using this policy	100
Policy details	100
Policy version	100
JSON policy document	100
Learn more	103
AmazonAugmentedAIFullAccess	104
Using this policy	104
Policy details	104
Policy version	104
JSON policy document	104
Learn more	105
AmazonAugmentedAIHumanLoopFullAccess	106
Using this policy	106
Policy details	106
Policy version	106
JSON policy document	106
Learn more	107

AmazonAugmentedAllIntegratedAPIAccess	107
Using this policy	107
Policy details	107
Policy version	107
JSON policy document	108
Learn more	109
AmazonBedrockFullAccess	109
Using this policy	109
Policy details	109
Policy version	110
JSON policy document	110
Learn more	111
AmazonBedrockReadOnly	111
Using this policy	111
Policy details	111
Policy version	112
JSON policy document	112
Learn more	112
AmazonBraketFullAccess	113
Using this policy	113
Policy details	113
Policy version	113
JSON policy document	113
Learn more	117
AmazonBraketJobsExecutionPolicy	118
Using this policy	118
Policy details	118
Policy version	118
JSON policy document	118
Learn more	121
AmazonBraketServiceRolePolicy	121
Using this policy	121
Policy details	121
Policy version	121
JSON policy document	122
Learn more	122

AmazonChimeFullAccess	123
Using this policy	123
Policy details	123
Policy version	123
JSON policy document	123
Learn more	125
AmazonChimeReadOnly	126
Using this policy	126
Policy details	126
Policy version	126
JSON policy document	126
Learn more	127
AmazonChimeSDK	127
Using this policy	127
Policy details	127
Policy version	127
JSON policy document	128
Learn more	129
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	129
Using this policy	129
Policy details	129
Policy version	129
JSON policy document	129
Learn more	131
AmazonChimeSDKMessagingServiceRolePolicy	131
Using this policy	131
Policy details	131
Policy version	131
JSON policy document	132
Learn more	132
AmazonChimeServiceRolePolicy	132
Using this policy	133
Policy details	133
Policy version	133
JSON policy document	133
Learn more	134

AmazonChimeTranscriptionServiceLinkedRolePolicy	134
Using this policy	134
Policy details	134
Policy version	134
JSON policy document	135
Learn more	135
AmazonChimeUserManagement	135
Using this policy	135
Policy details	135
Policy version	136
JSON policy document	136
Learn more	137
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	137
Using this policy	137
Policy details	137
Policy version	138
JSON policy document	138
Learn more	140
AmazonCloudDirectoryFullAccess	140
Using this policy	140
Policy details	140
Policy version	140
JSON policy document	140
Learn more	141
AmazonCloudDirectoryReadOnlyAccess	141
Using this policy	141
Policy details	141
Policy version	142
JSON policy document	142
Learn more	142
AmazonCloudWatchEvidentlyFullAccess	142
Using this policy	143
Policy details	143
Policy version	143
JSON policy document	143
Learn more	146

AmazonCloudWatchEvidentlyReadOnlyAccess	146
Using this policy	146
Policy details	146
Policy version	146
JSON policy document	146
Learn more	147
AmazonCloudWatchEvidentlyServiceRolePolicy	147
Using this policy	147
Policy details	147
Policy version	148
JSON policy document	148
Learn more	149
AmazonCloudWatchRUMFullAccess	149
Using this policy	150
Policy details	150
Policy version	150
JSON policy document	150
Learn more	153
AmazonCloudWatchRUMReadOnlyAccess	153
Using this policy	153
Policy details	153
Policy version	153
JSON policy document	153
Learn more	154
AmazonCloudWatchRUMServiceRolePolicy	154
Using this policy	154
Policy details	154
Policy version	155
JSON policy document	155
Learn more	156
AmazonCodeCatalystFullAccess	156
Using this policy	156
Policy details	156
Policy version	156
JSON policy document	156
Learn more	157

AmazonCodeCatalystReadOnlyAccess	157
Using this policy	157
Policy details	158
Policy version	158
JSON policy document	158
Learn more	158
AmazonCodeCatalystSupportAccess	159
Using this policy	159
Policy details	159
Policy version	159
JSON policy document	159
Learn more	160
AmazonCodeGuruProfilerAgentAccess	160
Using this policy	160
Policy details	160
Policy version	161
JSON policy document	161
Learn more	161
AmazonCodeGuruProfilerFullAccess	161
Using this policy	162
Policy details	162
Policy version	162
JSON policy document	162
Learn more	163
AmazonCodeGuruProfilerReadOnlyAccess	163
Using this policy	163
Policy details	163
Policy version	163
JSON policy document	164
Learn more	164
AmazonCodeGuruReviewerFullAccess	164
Using this policy	165
Policy details	165
Policy version	165
JSON policy document	165
Learn more	168

AmazonCodeGuruReviewerReadOnlyAccess	168
Using this policy	168
Policy details	168
Policy version	168
JSON policy document	168
Learn more	169
AmazonCodeGuruReviewerServiceRolePolicy	169
Using this policy	169
Policy details	169
Policy version	170
JSON policy document	170
Learn more	172
AmazonCodeGuruSecurityFullAccess	172
Using this policy	172
Policy details	172
Policy version	172
JSON policy document	173
Learn more	173
AmazonCodeGuruSecurityScanAccess	173
Using this policy	173
Policy details	174
Policy version	174
JSON policy document	174
Learn more	174
AmazonCognitoDeveloperAuthenticatedIdentities	175
Using this policy	175
Policy details	175
Policy version	175
JSON policy document	175
Learn more	176
AmazonCognitoIamEmailServiceRolePolicy	176
Using this policy	176
Policy details	176
Policy version	177
JSON policy document	177
Learn more	177

AmazonCognitoDpServiceRolePolicy	177
Using this policy	178
Policy details	178
Policy version	178
JSON policy document	178
Learn more	179
AmazonCognitoPowerUser	179
Using this policy	179
Policy details	179
Policy version	179
JSON policy document	179
Learn more	181
AmazonCognitoReadOnly	181
Using this policy	181
Policy details	181
Policy version	181
JSON policy document	182
Learn more	182
AmazonCognitoUnAuthedIdentitiesSessionPolicy	182
Using this policy	183
Policy details	183
Policy version	183
JSON policy document	183
Learn more	184
AmazonCognitoUnauthenticatedIdentities	184
Using this policy	184
Policy details	184
Policy version	185
JSON policy document	185
Learn more	185
AmazonConnect_FullAccess	185
Using this policy	186
Policy details	186
Policy version	186
JSON policy document	186
Learn more	189

AmazonConnectCampaignsServiceLinkedRolePolicy	189
Using this policy	189
Policy details	189
Policy version	189
JSON policy document	190
Learn more	190
AmazonConnectReadOnlyAccess	190
Using this policy	190
Policy details	191
Policy version	191
JSON policy document	191
Learn more	192
AmazonConnectServiceLinkedRolePolicy	192
Using this policy	192
Policy details	192
Policy version	192
JSON policy document	192
Learn more	198
AmazonConnectSynchronizationServiceRolePolicy	198
Using this policy	198
Policy details	198
Policy version	198
JSON policy document	199
Learn more	201
AmazonConnectVoiceIDFullAccess	201
Using this policy	201
Policy details	201
Policy version	201
JSON policy document	201
Learn more	202
AmazonDataZoneDomainExecutionRolePolicy	202
Using this policy	202
Policy details	202
Policy version	202
JSON policy document	203
Learn more	206

AmazonDataZoneEnvironmentRolePermissionsBoundary	206
Using this policy	206
Policy details	206
Policy version	206
JSON policy document	207
Learn more	219
AmazonDataZoneFullAccess	220
Using this policy	220
Policy details	220
Policy version	220
JSON policy document	220
Learn more	224
AmazonDataZoneFullUserAccess	224
Using this policy	224
Policy details	225
Policy version	225
JSON policy document	225
Learn more	228
AmazonDataZoneGlueManageAccessRolePolicy	228
Using this policy	228
Policy details	228
Policy version	229
JSON policy document	229
Learn more	234
AmazonDataZonePortalFullAccessPolicy	234
Using this policy	234
Policy details	234
Policy version	235
JSON policy document	235
Learn more	235
AmazonDataZonePreviewConsoleFullAccess	235
Using this policy	235
Policy details	236
Policy version	236
JSON policy document	236
Learn more	238

AmazonDataZoneProjectDeploymentPermissionsBoundary	238
Using this policy	238
Policy details	238
Policy version	239
JSON policy document	239
Learn more	247
AmazonDataZoneProjectRolePermissionsBoundary	247
Using this policy	247
Policy details	247
Policy version	247
JSON policy document	248
Learn more	255
AmazonDataZoneRedshiftGlueProvisioningPolicy	255
Using this policy	255
Policy details	255
Policy version	256
JSON policy document	256
Learn more	263
AmazonDataZoneRedshiftManageAccessRolePolicy	264
Using this policy	264
Policy details	264
Policy version	264
JSON policy document	264
Learn more	266
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary	267
Using this policy	267
Policy details	267
Policy version	267
JSON policy document	267
Learn more	295
AmazonDataZoneSageMakerManageAccessRolePolicy	295
Using this policy	295
Policy details	295
Policy version	295
JSON policy document	296
Learn more	300

AmazonDataZoneSageMakerProvisioningRolePolicy	300
Using this policy	301
Policy details	301
Policy version	301
JSON policy document	301
Learn more	306
AmazonDetectiveFullAccess	306
Using this policy	306
Policy details	306
Policy version	306
JSON policy document	307
Learn more	307
AmazonDetectiveInvestigatorAccess	308
Using this policy	308
Policy details	308
Policy version	308
JSON policy document	308
Learn more	310
AmazonDetectiveMemberAccess	310
Using this policy	310
Policy details	310
Policy version	311
JSON policy document	311
Learn more	311
AmazonDetectiveOrganizationsAccess	312
Using this policy	312
Policy details	312
Policy version	312
JSON policy document	312
Learn more	314
AmazonDetectiveServiceLinkedRolePolicy	314
Using this policy	314
Policy details	314
Policy version	315
JSON policy document	315
Learn more	315

AmazonDevOpsGuruConsoleFullAccess	315
Using this policy	315
Policy details	316
Policy version	316
JSON policy document	316
Learn more	318
AmazonDevOpsGuruFullAccess	319
Using this policy	319
Policy details	319
Policy version	319
JSON policy document	319
Learn more	321
AmazonDevOpsGuruOrganizationsAccess	322
Using this policy	322
Policy details	322
Policy version	322
JSON policy document	322
Learn more	323
AmazonDevOpsGuruReadOnlyAccess	324
Using this policy	324
Policy details	324
Policy version	324
JSON policy document	324
Learn more	326
AmazonDevOpsGuruServiceRolePolicy	326
Using this policy	327
Policy details	327
Policy version	327
JSON policy document	327
Learn more	331
AmazonDMSCloudWatchLogsRole	331
Using this policy	331
Policy details	332
Policy version	332
JSON policy document	332
Learn more	333

AmazonDMSRedshiftS3Role	334
Using this policy	334
Policy details	334
Policy version	334
JSON policy document	334
Learn more	335
AmazonDMSVPCManagementRole	335
Using this policy	335
Policy details	335
Policy version	336
JSON policy document	336
Learn more	336
AmazonDocDB-ElasticServiceRolePolicy	337
Using this policy	337
Policy details	337
Policy version	337
JSON policy document	337
Learn more	338
AmazonDocDBConsoleFullAccess	338
Using this policy	338
Policy details	338
Policy version	338
JSON policy document	339
Learn more	343
AmazonDocDBElasticFullAccess	343
Using this policy	343
Policy details	343
Policy version	344
JSON policy document	344
Learn more	347
AmazonDocDBElasticReadOnlyAccess	347
Using this policy	347
Policy details	347
Policy version	347
JSON policy document	348
Learn more	348

AmazonDocDBFullAccess	349
Using this policy	349
Policy details	349
Policy version	349
JSON policy document	349
Learn more	352
AmazonDocDBReadOnlyAccess	352
Using this policy	352
Policy details	352
Policy version	353
JSON policy document	353
Learn more	355
AmazonDRSVPCManagement	355
Using this policy	355
Policy details	355
Policy version	355
JSON policy document	355
Learn more	356
AmazonDynamoDBFullAccess	356
Using this policy	356
Policy details	357
Policy version	357
JSON policy document	357
Learn more	360
AmazonDynamoDBFullAccesswithDataPipeline	360
Using this policy	360
Policy details	360
Policy version	360
JSON policy document	361
Learn more	363
AmazonDynamoDBReadOnlyAccess	363
Using this policy	363
Policy details	363
Policy version	363
JSON policy document	363
Learn more	365

AmazonEBSCSIDriverPolicy	365
Using this policy	365
Policy details	366
Policy version	366
JSON policy document	366
Learn more	369
AmazonEC2ContainerRegistryFullAccess	369
Using this policy	369
Policy details	370
Policy version	370
JSON policy document	370
Learn more	371
AmazonEC2ContainerRegistryPowerUser	371
Using this policy	371
Policy details	371
Policy version	371
JSON policy document	372
Learn more	372
AmazonEC2ContainerRegistryReadOnly	372
Using this policy	373
Policy details	373
Policy version	373
JSON policy document	373
Learn more	374
AmazonEC2ContainerServiceAutoscaleRole	374
Using this policy	374
Policy details	374
Policy version	374
JSON policy document	375
Learn more	375
AmazonEC2ContainerServiceEventsRole	376
Using this policy	376
Policy details	376
Policy version	376
JSON policy document	376
Learn more	377

AmazonEC2ContainerServiceforEC2Role	377
Using this policy	378
Policy details	378
Policy version	378
JSON policy document	378
Learn more	379
AmazonEC2ContainerServiceRole	379
Using this policy	379
Policy details	380
Policy version	380
JSON policy document	380
Learn more	380
AmazonEC2FullAccess	381
Using this policy	381
Policy details	381
Policy version	381
JSON policy document	381
Learn more	382
AmazonEC2ReadOnlyAccess	383
Using this policy	383
Policy details	383
Policy version	383
JSON policy document	383
Learn more	384
AmazonEC2RoleforAWSCodeDeploy	384
Using this policy	384
Policy details	384
Policy version	385
JSON policy document	385
Learn more	385
AmazonEC2RoleforAWSCodeDeployLimited	386
Using this policy	386
Policy details	386
Policy version	386
JSON policy document	386
Learn more	387

AmazonEC2RoleforDataPipelineRole	387
Using this policy	387
Policy details	387
Policy version	388
JSON policy document	388
Learn more	389
AmazonEC2RoleforSSM	389
Using this policy	389
Policy details	389
Policy version	389
JSON policy document	390
Learn more	392
AmazonEC2RolePolicyForLaunchWizard	392
Using this policy	392
Policy details	392
Policy version	392
JSON policy document	393
Learn more	397
AmazonEC2SpotFleetAutoscaleRole	397
Using this policy	397
Policy details	397
Policy version	397
JSON policy document	397
Learn more	398
AmazonEC2SpotFleetTaggingRole	399
Using this policy	399
Policy details	399
Policy version	399
JSON policy document	399
Learn more	401
AmazonECS_FullAccess	401
Using this policy	401
Policy details	401
Policy version	401
JSON policy document	401
Learn more	407

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	407
Using this policy	407
Policy details	407
Policy version	408
JSON policy document	408
Learn more	410
AmazonECSInfrastructureRolePolicyForVolumes	410
Using this policy	410
Policy details	410
Policy version	411
JSON policy document	411
Learn more	413
AmazonECSServiceRolePolicy	413
Using this policy	413
Policy details	413
Policy version	413
JSON policy document	414
Learn more	418
AmazonECSTaskExecutionRolePolicy	419
Using this policy	419
Policy details	419
Policy version	419
JSON policy document	419
Learn more	420
AmazonEFSCSIDriverPolicy	420
Using this policy	420
Policy details	420
Policy version	420
JSON policy document	421
Learn more	422
AmazonEKS_CNI_Policy	422
Using this policy	423
Policy details	423
Policy version	423
JSON policy document	423
Learn more	424

AmazonEKSClusterPolicy	424
Using this policy	424
Policy details	424
Policy version	425
JSON policy document	425
Learn more	427
AmazonEKSConectorServiceRolePolicy	427
Using this policy	427
Policy details	427
Policy version	428
JSON policy document	428
Learn more	430
AmazonEKSFargatePodExecutionRolePolicy	430
Using this policy	430
Policy details	430
Policy version	430
JSON policy document	430
Learn more	431
AmazonEKSFargateServiceRolePolicy	431
Using this policy	431
Policy details	431
Policy version	432
JSON policy document	432
Learn more	432
AmazonEKSLocalOutpostClusterPolicy	432
Using this policy	433
Policy details	433
Policy version	433
JSON policy document	433
Learn more	435
AmazonEKSLocalOutpostServiceRolePolicy	435
Using this policy	435
Policy details	435
Policy version	436
JSON policy document	436
Learn more	441

AmazonEKSServicePolicy	441
Using this policy	442
Policy details	442
Policy version	442
JSON policy document	442
Learn more	444
AmazonEKSServiceRolePolicy	444
Using this policy	444
Policy details	444
Policy version	444
JSON policy document	445
Learn more	447
AmazonEKSVPCResourceController	447
Using this policy	447
Policy details	447
Policy version	448
JSON policy document	448
Learn more	448
AmazonEKSWorkerNodePolicy	449
Using this policy	449
Policy details	449
Policy version	449
JSON policy document	449
Learn more	450
AmazonElasticCacheFullAccess	450
Using this policy	450
Policy details	450
Policy version	451
JSON policy document	451
Learn more	454
AmazonElasticCacheReadOnlyAccess	454
Using this policy	454
Policy details	454
Policy version	455
JSON policy document	455
Learn more	455

AmazonElasticContainerRegistryPublicFullAccess	455
Using this policy	456
Policy details	456
Policy version	456
JSON policy document	456
Learn more	457
AmazonElasticContainerRegistryPublicPowerUser	457
Using this policy	457
Policy details	457
Policy version	457
JSON policy document	457
Learn more	458
AmazonElasticContainerRegistryPublicReadOnly	458
Using this policy	459
Policy details	459
Policy version	459
JSON policy document	459
Learn more	460
AmazonElasticFileSystemClientFullAccess	460
Using this policy	460
Policy details	460
Policy version	460
JSON policy document	461
Learn more	461
AmazonElasticFileSystemClientReadOnlyAccess	461
Using this policy	461
Policy details	461
Policy version	462
JSON policy document	462
Learn more	462
AmazonElasticFileSystemClientReadWriteAccess	462
Using this policy	463
Policy details	463
Policy version	463
JSON policy document	463
Learn more	464

AmazonElasticFileSystemFullAccess	464
Using this policy	464
Policy details	464
Policy version	464
JSON policy document	464
Learn more	466
AmazonElasticFileSystemReadOnlyAccess	466
Using this policy	466
Policy details	467
Policy version	467
JSON policy document	467
Learn more	468
AmazonElasticFileSystemServiceRolePolicy	468
Using this policy	468
Policy details	468
Policy version	469
JSON policy document	469
Learn more	471
AmazonElasticFileSystemsUtils	471
Using this policy	471
Policy details	471
Policy version	471
JSON policy document	472
Learn more	473
AmazonElasticMapReduceEditorsRole	474
Using this policy	474
Policy details	474
Policy version	474
JSON policy document	474
Learn more	475
AmazonElasticMapReduceforAutoScalingRole	476
Using this policy	476
Policy details	476
Policy version	476
JSON policy document	476
Learn more	477

AmazonElasticMapReduceforEC2Role	477
Using this policy	477
Policy details	477
Policy version	477
JSON policy document	478
Learn more	479
AmazonElasticMapReduceFullAccess	479
Using this policy	479
Policy details	479
Policy version	480
JSON policy document	480
Learn more	481
AmazonElasticMapReducePlacementGroupPolicy	482
Using this policy	482
Policy details	482
Policy version	482
JSON policy document	482
Learn more	483
AmazonElasticMapReduceReadOnlyAccess	483
Using this policy	483
Policy details	483
Policy version	484
JSON policy document	484
Learn more	484
AmazonElasticMapReduceRole	485
Using this policy	485
Policy details	485
Policy version	485
JSON policy document	485
Learn more	487
AmazonElasticsearchServiceRolePolicy	488
Using this policy	488
Policy details	488
Policy version	488
JSON policy document	488
Learn more	491

AmazonElasticTranscoder_FullAccess	491
Using this policy	491
Policy details	491
Policy version	492
JSON policy document	492
Learn more	493
AmazonElasticTranscoder_JobsSubmitter	493
Using this policy	493
Policy details	493
Policy version	493
JSON policy document	494
Learn more	494
AmazonElasticTranscoder_ReadOnlyAccess	494
Using this policy	494
Policy details	495
Policy version	495
JSON policy document	495
Learn more	495
AmazonElasticTranscoderRole	496
Using this policy	496
Policy details	496
Policy version	496
JSON policy document	496
Learn more	497
AmazonEMRCleanupPolicy	497
Using this policy	497
Policy details	498
Policy version	498
JSON policy document	498
Learn more	499
AmazonEMRContainersServiceRolePolicy	499
Using this policy	499
Policy details	499
Policy version	499
JSON policy document	500
Learn more	501

AmazonEMRFullAccessPolicy_v2	501
Using this policy	501
Policy details	501
Policy version	501
JSON policy document	502
Learn more	505
AmazonEMRReadOnlyAccessPolicy_v2	505
Using this policy	505
Policy details	505
Policy version	506
JSON policy document	506
Learn more	507
AmazonEMRServerlessServiceRolePolicy	507
Using this policy	507
Policy details	507
Policy version	507
JSON policy document	508
Learn more	509
AmazonEMRServicePolicy_v2	509
Using this policy	509
Policy details	509
Policy version	509
JSON policy document	509
Learn more	517
AmazonESCognitoAccess	517
Using this policy	517
Policy details	517
Policy version	518
JSON policy document	518
Learn more	519
AmazonESFullAccess	519
Using this policy	519
Policy details	519
Policy version	519
JSON policy document	520
Learn more	520

AmazonESReadOnlyAccess	520
Using this policy	520
Policy details	520
Policy version	521
JSON policy document	521
Learn more	521
AmazonEventBridgeApiDestinationsServiceRolePolicy	522
Using this policy	522
Policy details	522
Policy version	522
JSON policy document	522
Learn more	523
AmazonEventBridgeFullAccess	523
Using this policy	523
Policy details	523
Policy version	523
JSON policy document	524
Learn more	526
AmazonEventBridgePipesFullAccess	526
Using this policy	526
Policy details	526
Policy version	526
JSON policy document	526
Learn more	527
AmazonEventBridgePipesOperatorAccess	527
Using this policy	527
Policy details	528
Policy version	528
JSON policy document	528
Learn more	528
AmazonEventBridgePipesReadOnlyAccess	529
Using this policy	529
Policy details	529
Policy version	529
JSON policy document	529
Learn more	530

AmazonEventBridgeReadOnlyAccess	530
Using this policy	530
Policy details	530
Policy version	530
JSON policy document	531
Learn more	532
AmazonEventBridgeSchedulerFullAccess	532
Using this policy	532
Policy details	532
Policy version	533
JSON policy document	533
Learn more	533
AmazonEventBridgeSchedulerReadOnlyAccess	534
Using this policy	534
Policy details	534
Policy version	534
JSON policy document	534
Learn more	535
AmazonEventBridgeSchemasFullAccess	535
Using this policy	535
Policy details	535
Policy version	535
JSON policy document	536
Learn more	536
AmazonEventBridgeSchemasReadOnlyAccess	537
Using this policy	537
Policy details	537
Policy version	537
JSON policy document	537
Learn more	538
AmazonEventBridgeSchemasServiceRolePolicy	538
Using this policy	538
Policy details	538
Policy version	539
JSON policy document	539
Learn more	539

AmazonFISServiceRolePolicy	540
Using this policy	540
Policy details	540
Policy version	540
JSON policy document	540
Learn more	542
AmazonForecastFullAccess	542
Using this policy	542
Policy details	542
Policy version	542
JSON policy document	543
Learn more	543
AmazonFraudDetectorFullAccessPolicy	544
Using this policy	544
Policy details	544
Policy version	544
JSON policy document	544
Learn more	545
AmazonFreeRTOSFullAccess	546
Using this policy	546
Policy details	546
Policy version	546
JSON policy document	546
Learn more	547
AmazonFreeRTOSOTAUpdate	547
Using this policy	547
Policy details	547
Policy version	547
JSON policy document	547
Learn more	549
AmazonFSxConsoleFullAccess	549
Using this policy	549
Policy details	549
Policy version	549
JSON policy document	550
Learn more	553

AmazonFSxConsoleReadOnlyAccess	553
Using this policy	553
Policy details	553
Policy version	554
JSON policy document	554
Learn more	555
AmazonFSxFullAccess	555
Using this policy	555
Policy details	555
Policy version	555
JSON policy document	555
Learn more	559
AmazonFSxReadOnlyAccess	560
Using this policy	560
Policy details	560
Policy version	560
JSON policy document	560
Learn more	561
AmazonFSxServiceRolePolicy	561
Using this policy	561
Policy details	561
Policy version	561
JSON policy document	562
Learn more	564
AmazonGlacierFullAccess	564
Using this policy	565
Policy details	565
Policy version	565
JSON policy document	565
Learn more	565
AmazonGlacierReadOnlyAccess	566
Using this policy	566
Policy details	566
Policy version	566
JSON policy document	566
Learn more	567

AmazonGrafanaAthenaAccess	567
Using this policy	567
Policy details	567
Policy version	568
JSON policy document	568
Learn more	569
AmazonGrafanaCloudWatchAccess	570
Using this policy	570
Policy details	570
Policy version	570
JSON policy document	570
Learn more	572
AmazonGrafanaRedshiftAccess	572
Using this policy	572
Policy details	572
Policy version	572
JSON policy document	573
Learn more	574
AmazonGrafanaServiceLinkedRolePolicy	574
Using this policy	574
Policy details	574
Policy version	575
JSON policy document	575
Learn more	576
AmazonGuardDutyFullAccess	576
Using this policy	576
Policy details	576
Policy version	577
JSON policy document	577
Learn more	578
AmazonGuardDutyMalwareProtectionServiceRolePolicy	578
Using this policy	579
Policy details	579
Policy version	579
JSON policy document	579
Learn more	584

AmazonGuardDutyReadOnlyAccess	584
Using this policy	584
Policy details	584
Policy version	584
JSON policy document	584
Learn more	585
AmazonGuardDutyServiceRolePolicy	585
Using this policy	586
Policy details	586
Policy version	586
JSON policy document	586
Learn more	592
AmazonHealthLakeFullAccess	592
Using this policy	592
Policy details	592
Policy version	593
JSON policy document	593
Learn more	594
AmazonHealthLakeReadOnlyAccess	594
Using this policy	594
Policy details	594
Policy version	594
JSON policy document	594
Learn more	595
AmazonHoneycodeFullAccess	595
Using this policy	595
Policy details	595
Policy version	596
JSON policy document	596
Learn more	596
AmazonHoneycodeReadOnlyAccess	596
Using this policy	597
Policy details	597
Policy version	597
JSON policy document	597
Learn more	598

AmazonHoneycodeServiceRolePolicy	598
Using this policy	598
Policy details	598
Policy version	598
JSON policy document	598
Learn more	599
AmazonHoneycodeTeamAssociationFullAccess	599
Using this policy	599
Policy details	599
Policy version	600
JSON policy document	600
Learn more	600
AmazonHoneycodeTeamAssociationReadOnlyAccess	600
Using this policy	601
Policy details	601
Policy version	601
JSON policy document	601
Learn more	601
AmazonHoneycodeWorkbookFullAccess	602
Using this policy	602
Policy details	602
Policy version	602
JSON policy document	602
Learn more	603
AmazonHoneycodeWorkbookReadOnlyAccess	603
Using this policy	603
Policy details	603
Policy version	604
JSON policy document	604
Learn more	604
AmazonInspector2AgentlessServiceRolePolicy	605
Using this policy	605
Policy details	605
Policy version	605
JSON policy document	605
Learn more	609

AmazonInspector2FullAccess	609
Using this policy	609
Policy details	609
Policy version	609
JSON policy document	610
Learn more	611
AmazonInspector2ManagedCisPolicy	611
Using this policy	611
Policy details	611
Policy version	612
JSON policy document	612
Learn more	612
AmazonInspector2ReadOnlyAccess	612
Using this policy	613
Policy details	613
Policy version	613
JSON policy document	613
Learn more	614
AmazonInspector2ServiceRolePolicy	614
Using this policy	614
Policy details	614
Policy version	614
JSON policy document	615
Learn more	621
AmazonInspectorFullAccess	621
Using this policy	621
Policy details	621
Policy version	622
JSON policy document	622
Learn more	623
AmazonInspectorReadOnlyAccess	623
Using this policy	623
Policy details	623
Policy version	623
JSON policy document	624
Learn more	624

AmazonInspectorServiceRolePolicy	624
Using this policy	625
Policy details	625
Policy version	625
JSON policy document	625
Learn more	626
AmazonKendraFullAccess	627
Using this policy	627
Policy details	627
Policy version	627
JSON policy document	627
Learn more	629
AmazonKendraReadOnlyAccess	629
Using this policy	629
Policy details	629
Policy version	630
JSON policy document	630
Learn more	630
AmazonKeyspacesFullAccess	631
Using this policy	631
Policy details	631
Policy version	631
JSON policy document	631
Learn more	633
AmazonKeyspacesReadOnlyAccess	633
Using this policy	633
Policy details	633
Policy version	634
JSON policy document	634
Learn more	635
AmazonKeyspacesReadOnlyAccess_v2	635
Using this policy	635
Policy details	635
Policy version	635
JSON policy document	635
Learn more	636

AmazonKinesisAnalyticsFullAccess	636
Using this policy	637
Policy details	637
Policy version	637
JSON policy document	637
Learn more	638
AmazonKinesisAnalyticsReadOnly	639
Using this policy	639
Policy details	639
Policy version	639
JSON policy document	639
Learn more	641
AmazonKinesisFirehoseFullAccess	641
Using this policy	641
Policy details	641
Policy version	641
JSON policy document	641
Learn more	642
AmazonKinesisFirehoseReadOnlyAccess	642
Using this policy	642
Policy details	642
Policy version	643
JSON policy document	643
Learn more	643
AmazonKinesisFullAccess	643
Using this policy	643
Policy details	644
Policy version	644
JSON policy document	644
Learn more	644
AmazonKinesisReadOnlyAccess	645
Using this policy	645
Policy details	645
Policy version	645
JSON policy document	645
Learn more	646

AmazonKinesisVideoStreamsFullAccess	646
Using this policy	646
Policy details	646
Policy version	646
JSON policy document	647
Learn more	647
AmazonKinesisVideoStreamsReadOnlyAccess	647
Using this policy	647
Policy details	647
Policy version	648
JSON policy document	648
Learn more	648
AmazonLaunchWizard_Fullaccess	648
Using this policy	649
Policy details	649
Policy version	649
JSON policy document	649
Learn more	663
AmazonLaunchWizardFullAccessV2	663
Using this policy	664
Policy details	664
Policy version	664
JSON policy document	664
Learn more	681
AmazonLexChannelsAccess	681
Using this policy	681
Policy details	681
Policy version	681
JSON policy document	681
Learn more	682
AmazonLexFullAccess	682
Using this policy	682
Policy details	682
Policy version	682
JSON policy document	683
Learn more	688

AmazonLexReadOnly	688
Using this policy	688
Policy details	689
Policy version	689
JSON policy document	689
Learn more	690
AmazonLexReplicationPolicy	691
Using this policy	691
Policy details	691
Policy version	691
JSON policy document	691
Learn more	694
AmazonLexRunBotsOnly	694
Using this policy	694
Policy details	694
Policy version	694
JSON policy document	694
Learn more	695
AmazonLexV2BotPolicy	695
Using this policy	695
Policy details	695
Policy version	696
JSON policy document	696
Learn more	696
AmazonLookoutEquipmentFullAccess	696
Using this policy	696
Policy details	697
Policy version	697
JSON policy document	697
Learn more	698
AmazonLookoutEquipmentReadOnlyAccess	698
Using this policy	698
Policy details	699
Policy version	699
JSON policy document	699
Learn more	699

AmazonLookoutMetricsFullAccess	700
Using this policy	700
Policy details	700
Policy version	700
JSON policy document	700
Learn more	701
AmazonLookoutMetricsReadOnlyAccess	701
Using this policy	701
Policy details	701
Policy version	702
JSON policy document	702
Learn more	702
AmazonLookoutVisionConsoleFullAccess	703
Using this policy	703
Policy details	703
Policy version	703
JSON policy document	703
Learn more	705
AmazonLookoutVisionConsoleReadOnlyAccess	706
Using this policy	706
Policy details	706
Policy version	706
JSON policy document	706
Learn more	708
AmazonLookoutVisionFullAccess	708
Using this policy	708
Policy details	708
Policy version	708
JSON policy document	709
Learn more	709
AmazonLookoutVisionReadOnlyAccess	709
Using this policy	709
Policy details	709
Policy version	710
JSON policy document	710
Learn more	710

AmazonMachineLearningBatchPredictionsAccess	711
Using this policy	711
Policy details	711
Policy version	711
JSON policy document	711
Learn more	712
AmazonMachineLearningCreateOnlyAccess	712
Using this policy	712
Policy details	712
Policy version	712
JSON policy document	713
Learn more	713
AmazonMachineLearningFullAccess	713
Using this policy	713
Policy details	713
Policy version	714
JSON policy document	714
Learn more	714
AmazonMachineLearningManageRealTimeEndpointOnlyAccess	714
Using this policy	715
Policy details	715
Policy version	715
JSON policy document	715
Learn more	716
AmazonMachineLearningReadOnlyAccess	716
Using this policy	716
Policy details	716
Policy version	716
JSON policy document	716
Learn more	717
AmazonMachineLearningRealTimePredictionOnlyAccess	717
Using this policy	717
Policy details	717
Policy version	718
JSON policy document	718
Learn more	718

AmazonMachineLearningRoleforRedshiftDataSourceV3	718
Using this policy	719
Policy details	719
Policy version	719
JSON policy document	719
Learn more	720
AmazonMacieFullAccess	720
Using this policy	720
Policy details	720
Policy version	721
JSON policy document	721
Learn more	722
AmazonMacieHandshakeRole	722
Using this policy	722
Policy details	722
Policy version	722
JSON policy document	722
Learn more	723
AmazonMacieReadOnlyAccess	723
Using this policy	723
Policy details	723
Policy version	724
JSON policy document	724
Learn more	724
AmazonMacieServiceRole	724
Using this policy	725
Policy details	725
Policy version	725
JSON policy document	725
Learn more	725
AmazonMacieServiceRolePolicy	726
Using this policy	726
Policy details	726
Policy version	726
JSON policy document	726
Learn more	728

AmazonManagedBlockchainConsoleFullAccess	728
Using this policy	728
Policy details	728
Policy version	728
JSON policy document	728
Learn more	729
AmazonManagedBlockchainFullAccess	729
Using this policy	729
Policy details	729
Policy version	730
JSON policy document	730
Learn more	730
AmazonManagedBlockchainReadOnlyAccess	730
Using this policy	731
Policy details	731
Policy version	731
JSON policy document	731
Learn more	732
AmazonManagedBlockchainServiceRolePolicy	732
Using this policy	732
Policy details	732
Policy version	732
JSON policy document	733
Learn more	733
AmazonMCSFullAccess	733
Using this policy	733
Policy details	734
Policy version	734
JSON policy document	734
Learn more	735
AmazonMCSReadOnlyAccess	735
Using this policy	736
Policy details	736
Policy version	736
JSON policy document	736
Learn more	737

AmazonMechanicalTurkFullAccess	737
Using this policy	737
Policy details	737
Policy version	737
JSON policy document	738
Learn more	738
AmazonMechanicalTurkReadOnly	738
Using this policy	738
Policy details	738
Policy version	739
JSON policy document	739
Learn more	739
AmazonMemoryDBFullAccess	739
Using this policy	740
Policy details	740
Policy version	740
JSON policy document	740
Learn more	741
AmazonMemoryDBReadOnlyAccess	741
Using this policy	741
Policy details	741
Policy version	741
JSON policy document	742
Learn more	742
AmazonMobileAnalyticsFinancialReportAccess	742
Using this policy	742
Policy details	742
Policy version	743
JSON policy document	743
Learn more	743
AmazonMobileAnalyticsFullAccess	743
Using this policy	744
Policy details	744
Policy version	744
JSON policy document	744
Learn more	744

AmazonMobileAnalyticsNon-financialReportAccess	745
Using this policy	745
Policy details	745
Policy version	745
JSON policy document	745
Learn more	746
AmazonMobileAnalyticsWriteOnlyAccess	746
Using this policy	746
Policy details	746
Policy version	746
JSON policy document	747
Learn more	747
AmazonMonitronFullAccess	747
Using this policy	747
Policy details	747
Policy version	748
JSON policy document	748
Learn more	750
AmazonMQApiFullAccess	750
Using this policy	750
Policy details	750
Policy version	750
JSON policy document	750
Learn more	751
AmazonMQApiReadOnlyAccess	752
Using this policy	752
Policy details	752
Policy version	752
JSON policy document	752
Learn more	753
AmazonMQFullAccess	753
Using this policy	753
Policy details	753
Policy version	753
JSON policy document	754
Learn more	755

AmazonMQReadOnlyAccess	755
Using this policy	755
Policy details	755
Policy version	755
JSON policy document	756
Learn more	756
AmazonMQServiceRolePolicy	756
Using this policy	757
Policy details	757
Policy version	757
JSON policy document	757
Learn more	759
AmazonMSKConnectReadOnlyAccess	759
Using this policy	759
Policy details	759
Policy version	759
JSON policy document	760
Learn more	761
AmazonMSKFullAccess	761
Using this policy	761
Policy details	761
Policy version	761
JSON policy document	762
Learn more	764
AmazonMSKReadOnlyAccess	765
Using this policy	765
Policy details	765
Policy version	765
JSON policy document	765
Learn more	766
AmazonMWAAServiceRolePolicy	766
Using this policy	766
Policy details	766
Policy version	766
JSON policy document	767
Learn more	769

AmazonNimbleStudio-LaunchProfileWorker	769
Using this policy	769
Policy details	769
Policy version	769
JSON policy document	770
Learn more	770
AmazonNimbleStudio-StudioAdmin	771
Using this policy	771
Policy details	771
Policy version	771
JSON policy document	771
Learn more	773
AmazonNimbleStudio-StudioUser	773
Using this policy	773
Policy details	774
Policy version	774
JSON policy document	774
Learn more	776
AmazonOmicsFullAccess	776
Using this policy	776
Policy details	776
Policy version	777
JSON policy document	777
Learn more	778
AmazonOmicsReadOnlyAccess	778
Using this policy	778
Policy details	778
Policy version	778
JSON policy document	779
Learn more	779
AmazonOneEnterpriseFullAccess	779
Using this policy	779
Policy details	780
Policy version	780
JSON policy document	780
Learn more	780

AmazonOneEnterpriseInstallerAccess	781
Using this policy	781
Policy details	781
Policy version	781
JSON policy document	781
Learn more	782
AmazonOneEnterpriseReadOnlyAccess	782
Using this policy	782
Policy details	782
Policy version	782
JSON policy document	783
Learn more	783
AmazonOpenSearchDashboardsServiceRolePolicy	783
Using this policy	783
Policy details	784
Policy version	784
JSON policy document	784
Learn more	784
AmazonOpenSearchDirectQueryGlueCreateAccess	785
Using this policy	785
Policy details	785
Policy version	785
JSON policy document	785
Learn more	786
AmazonOpenSearchIngestionFullAccess	786
Using this policy	786
Policy details	786
Policy version	786
JSON policy document	787
Learn more	788
AmazonOpenSearchIngestionReadOnlyAccess	788
Using this policy	788
Policy details	788
Policy version	788
JSON policy document	788
Learn more	789

AmazonOpenSearchIngestionServiceRolePolicy	789
Using this policy	789
Policy details	789
Policy version	790
JSON policy document	790
Learn more	792
AmazonOpenSearchServerlessServiceRolePolicy	792
Using this policy	792
Policy details	792
Policy version	792
JSON policy document	793
Learn more	793
AmazonOpenSearchServiceCognitoAccess	793
Using this policy	793
Policy details	793
Policy version	794
JSON policy document	794
Learn more	795
AmazonOpenSearchServiceFullAccess	795
Using this policy	795
Policy details	795
Policy version	796
JSON policy document	796
Learn more	796
AmazonOpenSearchServiceReadOnlyAccess	796
Using this policy	796
Policy details	797
Policy version	797
JSON policy document	797
Learn more	797
AmazonOpenSearchServiceRolePolicy	798
Using this policy	798
Policy details	798
Policy version	798
JSON policy document	798
Learn more	803

AmazonPersonalizeFullAccess	803
Using this policy	803
Policy details	803
Policy version	803
JSON policy document	804
Learn more	805
AmazonPollyFullAccess	805
Using this policy	805
Policy details	805
Policy version	805
JSON policy document	806
Learn more	806
AmazonPollyReadOnlyAccess	806
Using this policy	806
Policy details	807
Policy version	807
JSON policy document	807
Learn more	807
AmazonPrometheusConsoleFullAccess	808
Using this policy	808
Policy details	808
Policy version	808
JSON policy document	808
Learn more	809
AmazonPrometheusFullAccess	810
Using this policy	810
Policy details	810
Policy version	810
JSON policy document	810
Learn more	811
AmazonPrometheusQueryAccess	811
Using this policy	812
Policy details	812
Policy version	812
JSON policy document	812
Learn more	813

AmazonPrometheusRemoteWriteAccess	813
Using this policy	813
Policy details	813
Policy version	813
JSON policy document	813
Learn more	814
AmazonPrometheusScraperServiceRolePolicy	814
Using this policy	814
Policy details	814
Policy version	815
JSON policy document	815
Learn more	817
AmazonQFullAccess	817
Using this policy	817
Policy details	817
Policy version	818
JSON policy document	818
Learn more	818
AmazonQLDBConsoleFullAccess	819
Using this policy	819
Policy details	819
Policy version	819
JSON policy document	819
Learn more	821
AmazonQLDBFullAccess	821
Using this policy	821
Policy details	821
Policy version	822
JSON policy document	822
Learn more	823
AmazonQLDBReadOnly	823
Using this policy	823
Policy details	824
Policy version	824
JSON policy document	824
Learn more	825

AmazonRDSBetaServiceRolePolicy	825
Using this policy	825
Policy details	825
Policy version	825
JSON policy document	825
Learn more	829
AmazonRDSCustomInstanceProfileRolePolicy	829
Using this policy	829
Policy details	829
Policy version	829
JSON policy document	829
Learn more	837
AmazonRDSCustomPreviewServiceRolePolicy	837
Using this policy	837
Policy details	837
Policy version	837
JSON policy document	837
Learn more	853
AmazonRDSCustomServiceRolePolicy	853
Using this policy	853
Policy details	853
Policy version	854
JSON policy document	854
Learn more	871
AmazonRDSDataFullAccess	871
Using this policy	871
Policy details	872
Policy version	872
JSON policy document	872
Learn more	873
AmazonRDSDirectoryServiceAccess	873
Using this policy	873
Policy details	874
Policy version	874
JSON policy document	874
Learn more	874

AmazonRDSEnhancedMonitoringRole	875
Using this policy	875
Policy details	875
Policy version	875
JSON policy document	875
Learn more	876
AmazonRDSFullAccess	876
Using this policy	876
Policy details	876
Policy version	877
JSON policy document	877
Learn more	879
AmazonRDSPerformanceInsightsFullAccess	879
Using this policy	879
Policy details	879
Policy version	880
JSON policy document	880
Learn more	881
AmazonRDSPerformanceInsightsReadOnly	881
Using this policy	882
Policy details	882
Policy version	882
JSON policy document	882
Learn more	884
AmazonRDSPreviewServiceRolePolicy	884
Using this policy	884
Policy details	884
Policy version	884
JSON policy document	885
Learn more	888
AmazonRDSReadOnlyAccess	888
Using this policy	888
Policy details	888
Policy version	888
JSON policy document	889
Learn more	890

AmazonRDSServiceRolePolicy	890
Using this policy	890
Policy details	890
Policy version	890
JSON policy document	891
Learn more	895
AmazonRedshiftAllCommandsFullAccess	895
Using this policy	895
Policy details	895
Policy version	895
JSON policy document	895
Learn more	901
AmazonRedshiftDataFullAccess	901
Using this policy	901
Policy details	901
Policy version	901
JSON policy document	902
Learn more	904
AmazonRedshiftFullAccess	904
Using this policy	904
Policy details	904
Policy version	904
JSON policy document	904
Learn more	906
AmazonRedshiftQueryEditor	907
Using this policy	907
Policy details	907
Policy version	907
JSON policy document	907
Learn more	909
AmazonRedshiftQueryEditorV2FullAccess	909
Using this policy	910
Policy details	910
Policy version	910
JSON policy document	910
Learn more	911

AmazonRedshiftQueryEditorV2NoSharing	912
Using this policy	912
Policy details	912
Policy version	912
JSON policy document	912
Learn more	916
AmazonRedshiftQueryEditorV2ReadSharing	916
Using this policy	916
Policy details	916
Policy version	917
JSON policy document	917
Learn more	922
AmazonRedshiftQueryEditorV2ReadWriteSharing	922
Using this policy	922
Policy details	922
Policy version	922
JSON policy document	923
Learn more	928
AmazonRedshiftReadOnlyAccess	928
Using this policy	928
Policy details	928
Policy version	928
JSON policy document	928
Learn more	929
AmazonRedshiftServiceLinkedRolePolicy	929
Using this policy	930
Policy details	930
Policy version	930
JSON policy document	930
Learn more	935
AmazonRekognitionCustomLabelsFullAccess	936
Using this policy	936
Policy details	936
Policy version	936
JSON policy document	936
Learn more	937

AmazonRekognitionFullAccess	938
Using this policy	938
Policy details	938
Policy version	938
JSON policy document	938
Learn more	939
AmazonRekognitionReadOnlyAccess	939
Using this policy	939
Policy details	939
Policy version	939
JSON policy document	940
Learn more	941
AmazonRekognitionServiceRole	941
Using this policy	941
Policy details	941
Policy version	941
JSON policy document	942
Learn more	942
AmazonRoute53AutoNamingFullAccess	943
Using this policy	943
Policy details	943
Policy version	943
JSON policy document	943
Learn more	944
AmazonRoute53AutoNamingReadOnlyAccess	944
Using this policy	944
Policy details	944
Policy version	945
JSON policy document	945
Learn more	945
AmazonRoute53AutoNamingRegistrantAccess	945
Using this policy	946
Policy details	946
Policy version	946
JSON policy document	946
Learn more	947

AmazonRoute53DomainsFullAccess	947
Using this policy	947
Policy details	947
Policy version	947
JSON policy document	948
Learn more	948
AmazonRoute53DomainsReadOnlyAccess	948
Using this policy	948
Policy details	949
Policy version	949
JSON policy document	949
Learn more	949
AmazonRoute53FullAccess	950
Using this policy	950
Policy details	950
Policy version	950
JSON policy document	950
Learn more	951
AmazonRoute53ProfilesFullAccess	951
Using this policy	951
Policy details	952
Policy version	952
JSON policy document	952
Learn more	953
AmazonRoute53ProfilesReadOnlyAccess	953
Using this policy	953
Policy details	953
Policy version	954
JSON policy document	954
Learn more	954
AmazonRoute53ReadOnlyAccess	955
Using this policy	955
Policy details	955
Policy version	955
JSON policy document	955
Learn more	956

AmazonRoute53RecoveryClusterFullAccess	956
Using this policy	956
Policy details	956
Policy version	956
JSON policy document	957
Learn more	957
AmazonRoute53RecoveryClusterReadOnlyAccess	957
Using this policy	957
Policy details	957
Policy version	958
JSON policy document	958
Learn more	958
AmazonRoute53RecoveryControlConfigFullAccess	958
Using this policy	959
Policy details	959
Policy version	959
JSON policy document	959
Learn more	959
AmazonRoute53RecoveryControlConfigReadOnlyAccess	960
Using this policy	960
Policy details	960
Policy version	960
JSON policy document	960
Learn more	961
AmazonRoute53RecoveryReadinessFullAccess	961
Using this policy	961
Policy details	961
Policy version	962
JSON policy document	962
Learn more	962
AmazonRoute53RecoveryReadinessReadOnlyAccess	962
Using this policy	963
Policy details	963
Policy version	963
JSON policy document	963
Learn more	964

AmazonRoute53ResolverFullAccess	964
Using this policy	964
Policy details	964
Policy version	965
JSON policy document	965
Learn more	965
AmazonRoute53ResolverReadOnlyAccess	966
Using this policy	966
Policy details	966
Policy version	966
JSON policy document	966
Learn more	967
AmazonS3FullAccess	967
Using this policy	967
Policy details	967
Policy version	967
JSON policy document	968
Learn more	968
AmazonS3ObjectLambdaExecutionRolePolicy	968
Using this policy	968
Policy details	968
Policy version	969
JSON policy document	969
Learn more	969
AmazonS3OutpostsFullAccess	970
Using this policy	970
Policy details	970
Policy version	970
JSON policy document	970
Learn more	971
AmazonS3OutpostsReadOnlyAccess	971
Using this policy	972
Policy details	972
Policy version	972
JSON policy document	972
Learn more	973

AmazonS3ReadOnlyAccess	973
Using this policy	973
Policy details	974
Policy version	974
JSON policy document	974
Learn more	974
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	975
Using this policy	975
Policy details	975
Policy version	975
JSON policy document	975
Learn more	987
AmazonSageMakerCanvasAIServicesAccess	987
Using this policy	987
Policy details	987
Policy version	987
JSON policy document	988
Learn more	991
AmazonSageMakerCanvasBedrockAccess	991
Using this policy	991
Policy details	991
Policy version	991
JSON policy document	992
Learn more	992
AmazonSageMakerCanvasDataPrepFullAccess	993
Using this policy	993
Policy details	993
Policy version	993
JSON policy document	993
Learn more	1000
AmazonSageMakerCanvasDirectDeployAccess	1001
Using this policy	1001
Policy details	1001
Policy version	1001
JSON policy document	1001
Learn more	1002

AmazonSageMakerCanvasForecastAccess	1002
Using this policy	1002
Policy details	1003
Policy version	1003
JSON policy document	1003
Learn more	1004
AmazonSageMakerCanvasFullAccess	1004
Using this policy	1004
Policy details	1004
Policy version	1004
JSON policy document	1005
Learn more	1013
AmazonSageMakerClusterInstanceRolePolicy	1013
Using this policy	1013
Policy details	1013
Policy version	1013
JSON policy document	1013
Learn more	1015
AmazonSageMakerCoreServiceRolePolicy	1015
Using this policy	1016
Policy details	1016
Policy version	1016
JSON policy document	1016
Learn more	1017
AmazonSageMakerEdgeDeviceFleetPolicy	1017
Using this policy	1017
Policy details	1017
Policy version	1018
JSON policy document	1018
Learn more	1020
AmazonSageMakerFeatureStoreAccess	1020
Using this policy	1020
Policy details	1020
Policy version	1020
JSON policy document	1021
Learn more	1022

AmazonSageMakerFullAccess	1022
Using this policy	1022
Policy details	1022
Policy version	1022
JSON policy document	1022
Learn more	1038
AmazonSageMakerGeospatialExecutionRole	1039
Using this policy	1039
Policy details	1039
Policy version	1039
JSON policy document	1039
Learn more	1040
AmazonSageMakerGeospatialFullAccess	1040
Using this policy	1040
Policy details	1041
Policy version	1041
JSON policy document	1041
Learn more	1042
AmazonSageMakerGroundTruthExecution	1042
Using this policy	1042
Policy details	1042
Policy version	1042
JSON policy document	1043
Learn more	1046
AmazonSageMakerMechanicalTurkAccess	1046
Using this policy	1046
Policy details	1046
Policy version	1047
JSON policy document	1047
Learn more	1047
AmazonSageMakerModelGovernanceUseAccess	1048
Using this policy	1048
Policy details	1048
Policy version	1048
JSON policy document	1048
Learn more	1050

AmazonSageMakerModelRegistryFullAccess	1050
Using this policy	1050
Policy details	1051
Policy version	1051
JSON policy document	1051
Learn more	1055
AmazonSageMakerNotebooksServiceRolePolicy	1055
Using this policy	1055
Policy details	1055
Policy version	1055
JSON policy document	1055
Learn more	1059
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1060
Using this policy	1060
Policy details	1060
Policy version	1060
JSON policy document	1060
Learn more	1061
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1061
Using this policy	1062
Policy details	1062
Policy version	1062
JSON policy document	1062
Learn more	1066
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1066
Using this policy	1066
Policy details	1066
Policy version	1066
JSON policy document	1067
Learn more	1067
AmazonSageMakerPipelinesIntegrations	1067
Using this policy	1068
Policy details	1068
Policy version	1068
JSON policy document	1068
Learn more	1070

AmazonSageMakerReadOnly	1070
Using this policy	1070
Policy details	1070
Policy version	1071
JSON policy document	1071
Learn more	1072
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1072
Using this policy	1072
Policy details	1072
Policy version	1073
JSON policy document	1073
Learn more	1074
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1074
Using this policy	1074
Policy details	1074
Policy version	1074
JSON policy document	1075
Learn more	1081
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1082
Using this policy	1082
Policy details	1082
Policy version	1082
JSON policy document	1082
Learn more	1092
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1093
Using this policy	1093
Policy details	1093
Policy version	1093
JSON policy document	1093
Learn more	1096
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1096
Using this policy	1097
Policy details	1097
Policy version	1097
JSON policy document	1097
Learn more	1097

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1098
Using this policy	1098
Policy details	1098
Policy version	1098
JSON policy document	1098
Learn more	1099
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1099
Using this policy	1099
Policy details	1099
Policy version	1100
JSON policy document	1100
Learn more	1102
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1102
Using this policy	1102
Policy details	1103
Policy version	1103
JSON policy document	1103
Learn more	1113
AmazonSecurityLakeAdministrator	1113
Using this policy	1113
Policy details	1113
Policy version	1114
JSON policy document	1114
Learn more	1125
AmazonSecurityLakeMetastoreManager	1125
Using this policy	1125
Policy details	1125
Policy version	1126
JSON policy document	1126
Learn more	1128
AmazonSecurityLakePermissionsBoundary	1128
Using this policy	1128
Policy details	1129
Policy version	1129
JSON policy document	1129
Learn more	1132

AmazonSESEFullAccess	1132
Using this policy	1132
Policy details	1133
Policy version	1133
JSON policy document	1133
Learn more	1133
AmazonSESReadOnlyAccess	1134
Using this policy	1134
Policy details	1134
Policy version	1134
JSON policy document	1134
Learn more	1135
AmazonSESServiceRolePolicy	1135
Using this policy	1135
Policy details	1135
Policy version	1135
JSON policy document	1136
Learn more	1136
AmazonSNSFullAccess	1136
Using this policy	1136
Policy details	1136
Policy version	1137
JSON policy document	1137
Learn more	1137
AmazonSNSReadOnlyAccess	1137
Using this policy	1138
Policy details	1138
Policy version	1138
JSON policy document	1138
Learn more	1138
AmazonSNSRole	1139
Using this policy	1139
Policy details	1139
Policy version	1139
JSON policy document	1139
Learn more	1140

AmazonSQSFullAccess	1140
Using this policy	1140
Policy details	1140
Policy version	1141
JSON policy document	1141
Learn more	1141
AmazonSQSReadOnlyAccess	1141
Using this policy	1141
Policy details	1142
Policy version	1142
JSON policy document	1142
Learn more	1142
AmazonSSMAutomationApproverAccess	1143
Using this policy	1143
Policy details	1143
Policy version	1143
JSON policy document	1143
Learn more	1144
AmazonSSMAutomationRole	1144
Using this policy	1144
Policy details	1144
Policy version	1145
JSON policy document	1145
Learn more	1146
AmazonSSMDirectoryServiceAccess	1146
Using this policy	1147
Policy details	1147
Policy version	1147
JSON policy document	1147
Learn more	1147
AmazonSSMFullAccess	1148
Using this policy	1148
Policy details	1148
Policy version	1148
JSON policy document	1148
Learn more	1149

AmazonSSMMaintenanceWindowRole	1150
Using this policy	1150
Policy details	1150
Policy version	1150
JSON policy document	1150
Learn more	1152
AmazonSSMManagedEC2InstanceDefaultPolicy	1152
Using this policy	1152
Policy details	1152
Policy version	1152
JSON policy document	1153
Learn more	1154
AmazonSSMManagedInstanceCore	1154
Using this policy	1154
Policy details	1154
Policy version	1154
JSON policy document	1155
Learn more	1156
AmazonSSMPatchAssociation	1156
Using this policy	1156
Policy details	1156
Policy version	1157
JSON policy document	1157
Learn more	1157
AmazonSSMReadOnlyAccess	1158
Using this policy	1158
Policy details	1158
Policy version	1158
JSON policy document	1158
Learn more	1159
AmazonSSMServiceRolePolicy	1159
Using this policy	1159
Policy details	1159
Policy version	1159
JSON policy document	1160
Learn more	1165

AmazonSumerianFullAccess	1165
Using this policy	1165
Policy details	1165
Policy version	1165
JSON policy document	1165
Learn more	1166
AmazonTextractFullAccess	1166
Using this policy	1166
Policy details	1166
Policy version	1166
JSON policy document	1167
Learn more	1167
AmazonTextractServiceRole	1167
Using this policy	1167
Policy details	1167
Policy version	1168
JSON policy document	1168
Learn more	1168
AmazonTimestreamConsoleFullAccess	1168
Using this policy	1169
Policy details	1169
Policy version	1169
JSON policy document	1169
Learn more	1171
AmazonTimestreamFullAccess	1171
Using this policy	1171
Policy details	1171
Policy version	1172
JSON policy document	1172
Learn more	1173
AmazonTimestreamInfluxDBFullAccess	1173
Using this policy	1173
Policy details	1173
Policy version	1174
JSON policy document	1174
Learn more	1176

AmazonTimestreamInfluxDBServiceRolePolicy	1176
Using this policy	1176
Policy details	1176
Policy version	1176
JSON policy document	1177
Learn more	1179
AmazonTimestreamReadOnlyAccess	1179
Using this policy	1179
Policy details	1179
Policy version	1180
JSON policy document	1180
Learn more	1181
AmazonTranscribeFullAccess	1181
Using this policy	1181
Policy details	1181
Policy version	1181
JSON policy document	1181
Learn more	1182
AmazonTranscribeReadOnlyAccess	1182
Using this policy	1182
Policy details	1182
Policy version	1183
JSON policy document	1183
Learn more	1183
AmazonVPCCrossAccountNetworkInterfaceOperations	1183
Using this policy	1184
Policy details	1184
Policy version	1184
JSON policy document	1184
Learn more	1186
AmazonVPCFullAccess	1186
Using this policy	1186
Policy details	1186
Policy version	1186
JSON policy document	1186
Learn more	1190

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1190
Using this policy	1191
Policy details	1191
Policy version	1191
JSON policy document	1191
Learn more	1194
AmazonVPCReachabilityAnalyzerFullAccessPolicy	1195
Using this policy	1195
Policy details	1195
Policy version	1195
JSON policy document	1195
Learn more	1198
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1199
Using this policy	1199
Policy details	1199
Policy version	1199
JSON policy document	1199
Learn more	1200
AmazonVPCReadOnlyAccess	1200
Using this policy	1200
Policy details	1200
Policy version	1200
JSON policy document	1201
Learn more	1202
AmazonWorkDocsFullAccess	1202
Using this policy	1202
Policy details	1202
Policy version	1203
JSON policy document	1203
Learn more	1203
AmazonWorkDocsReadOnlyAccess	1203
Using this policy	1204
Policy details	1204
Policy version	1204
JSON policy document	1204
Learn more	1205

AmazonWorkMailEventsServiceRolePolicy	1205
Using this policy	1205
Policy details	1205
Policy version	1205
JSON policy document	1206
Learn more	1206
AmazonWorkMailFullAccess	1206
Using this policy	1206
Policy details	1206
Policy version	1207
JSON policy document	1207
Learn more	1209
AmazonWorkMailMessageFlowFullAccess	1209
Using this policy	1209
Policy details	1209
Policy version	1209
JSON policy document	1210
Learn more	1210
AmazonWorkMailMessageFlowReadOnlyAccess	1210
Using this policy	1210
Policy details	1210
Policy version	1211
JSON policy document	1211
Learn more	1211
AmazonWorkMailReadOnlyAccess	1211
Using this policy	1212
Policy details	1212
Policy version	1212
JSON policy document	1212
Learn more	1213
AmazonWorkSpacesAdmin	1213
Using this policy	1213
Policy details	1213
Policy version	1213
JSON policy document	1214
Learn more	1215

AmazonWorkSpacesApplicationManagerAdminAccess	1215
Using this policy	1215
Policy details	1215
Policy version	1215
JSON policy document	1216
Learn more	1216
AmazonWorkSpacesPCAAccess	1216
Using this policy	1216
Policy details	1216
Policy version	1217
JSON policy document	1217
Learn more	1217
AmazonWorkSpacesPoolServiceAccess	1218
Using this policy	1218
Policy details	1218
Policy version	1218
JSON policy document	1218
Learn more	1219
AmazonWorkSpacesSecureBrowserReadOnly	1220
Using this policy	1220
Policy details	1220
Policy version	1220
JSON policy document	1220
Learn more	1221
AmazonWorkSpacesSelfServiceAccess	1222
Using this policy	1222
Policy details	1222
Policy version	1222
JSON policy document	1222
Learn more	1223
AmazonWorkSpacesServiceAccess	1223
Using this policy	1223
Policy details	1223
Policy version	1223
JSON policy document	1224
Learn more	1224

AmazonWorkSpacesWebReadOnly	1224
Using this policy	1224
Policy details	1224
Policy version	1225
JSON policy document	1225
Learn more	1226
AmazonWorkSpacesWebServiceRolePolicy	1226
Using this policy	1226
Policy details	1226
Policy version	1227
JSON policy document	1227
Learn more	1229
AmazonZocaloFullAccess	1229
Using this policy	1229
Policy details	1229
Policy version	1230
JSON policy document	1230
Learn more	1230
AmazonZocaloReadOnlyAccess	1231
Using this policy	1231
Policy details	1231
Policy version	1231
JSON policy document	1231
Learn more	1232
AmplifyBackendDeployFullAccess	1232
Using this policy	1232
Policy details	1232
Policy version	1232
JSON policy document	1233
Learn more	1236
APIGatewayServiceRolePolicy	1237
Using this policy	1237
Policy details	1237
Policy version	1237
JSON policy document	1237
Learn more	1240

AppIntegrationsServiceLinkedRolePolicy	1240
Using this policy	1240
Policy details	1240
Policy version	1240
JSON policy document	1240
Learn more	1242
ApplicationAutoScalingForAmazonAppStreamAccess	1242
Using this policy	1242
Policy details	1242
Policy version	1243
JSON policy document	1243
Learn more	1243
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1244
Using this policy	1244
Policy details	1244
Policy version	1244
JSON policy document	1244
Learn more	1246
AppRunnerNetworkingServiceRolePolicy	1247
Using this policy	1247
Policy details	1247
Policy version	1247
JSON policy document	1247
Learn more	1249
AppRunnerServiceRolePolicy	1249
Using this policy	1249
Policy details	1249
Policy version	1249
JSON policy document	1249
Learn more	1250
AutoScalingConsoleFullAccess	1250
Using this policy	1251
Policy details	1251
Policy version	1251
JSON policy document	1251
Learn more	1253

AutoScalingConsoleReadOnlyAccess	1253
Using this policy	1253
Policy details	1253
Policy version	1253
JSON policy document	1254
Learn more	1255
AutoScalingFullAccess	1255
Using this policy	1255
Policy details	1255
Policy version	1255
JSON policy document	1256
Learn more	1257
AutoScalingNotificationAccessRole	1257
Using this policy	1257
Policy details	1257
Policy version	1258
JSON policy document	1258
Learn more	1258
AutoScalingReadOnlyAccess	1258
Using this policy	1259
Policy details	1259
Policy version	1259
JSON policy document	1259
Learn more	1259
AutoScalingServiceRolePolicy	1260
Using this policy	1260
Policy details	1260
Policy version	1260
JSON policy document	1260
Learn more	1263
AWS_ConfigRole	1263
Using this policy	1263
Policy details	1263
Policy version	1264
JSON policy document	1264
Learn more	1295

AWSAccountActivityAccess	1295
Using this policy	1295
Policy details	1295
Policy version	1295
JSON policy document	1295
Learn more	1296
AWSAccountManagementFullAccess	1296
Using this policy	1297
Policy details	1297
Policy version	1297
JSON policy document	1297
Learn more	1297
AWSAccountManagementReadOnlyAccess	1298
Using this policy	1298
Policy details	1298
Policy version	1298
JSON policy document	1298
Learn more	1299
AWSAccountUsageReportAccess	1299
Using this policy	1299
Policy details	1299
Policy version	1299
JSON policy document	1299
Learn more	1300
AWSAgentlessDiscoveryService	1300
Using this policy	1300
Policy details	1300
Policy version	1300
JSON policy document	1301
Learn more	1302
AWSAppFabricFullAccess	1303
Using this policy	1303
Policy details	1303
Policy version	1303
JSON policy document	1303
Learn more	1305

AWSAppFabricReadOnlyAccess	1305
Using this policy	1305
Policy details	1305
Policy version	1305
JSON policy document	1305
Learn more	1306
AWSAppFabricServiceRolePolicy	1306
Using this policy	1306
Policy details	1307
Policy version	1307
JSON policy document	1307
Learn more	1308
AWSApplicationAutoscalingAppStreamFleetPolicy	1308
Using this policy	1308
Policy details	1309
Policy version	1309
JSON policy document	1309
Learn more	1310
AWSApplicationAutoscalingCassandraTablePolicy	1310
Using this policy	1310
Policy details	1310
Policy version	1310
JSON policy document	1310
Learn more	1311
AWSApplicationAutoscalingComprehendEndpointPolicy	1311
Using this policy	1311
Policy details	1312
Policy version	1312
JSON policy document	1312
Learn more	1313
AWSApplicationAutoScalingCustomResourcePolicy	1313
Using this policy	1313
Policy details	1313
Policy version	1313
JSON policy document	1313
Learn more	1314

AWSApplicationAutoscalingDynamoDBTablePolicy	1314
Using this policy	1314
Policy details	1314
Policy version	1315
JSON policy document	1315
Learn more	1315
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1315
Using this policy	1316
Policy details	1316
Policy version	1316
JSON policy document	1316
Learn more	1317
AWSApplicationAutoscalingECSServicePolicy	1317
Using this policy	1317
Policy details	1317
Policy version	1317
JSON policy document	1318
Learn more	1318
AWSApplicationAutoscalingElastiCacheRGPolicy	1318
Using this policy	1318
Policy details	1319
Policy version	1319
JSON policy document	1319
Learn more	1320
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1320
Using this policy	1320
Policy details	1320
Policy version	1320
JSON policy document	1321
Learn more	1321
AWSApplicationAutoscalingKafkaClusterPolicy	1321
Using this policy	1321
Policy details	1322
Policy version	1322
JSON policy document	1322
Learn more	1323

AWSApplicationAutoscalingLambdaConcurrencyPolicy	1323
Using this policy	1323
Policy details	1323
Policy version	1323
JSON policy document	1323
Learn more	1324
AWSApplicationAutoscalingNeptuneClusterPolicy	1324
Using this policy	1324
Policy details	1324
Policy version	1325
JSON policy document	1325
Learn more	1326
AWSApplicationAutoscalingRDSClusterPolicy	1327
Using this policy	1327
Policy details	1327
Policy version	1327
JSON policy document	1327
Learn more	1328
AWSApplicationAutoscalingSageMakerEndpointPolicy	1328
Using this policy	1328
Policy details	1329
Policy version	1329
JSON policy document	1329
Learn more	1330
AWSApplicationAutoscalingWorkSpacesPoolPolicy	1330
Using this policy	1330
Policy details	1330
Policy version	1331
JSON policy document	1331
Learn more	1332
AWSApplicationDiscoveryAgentAccess	1332
Using this policy	1332
Policy details	1332
Policy version	1333
JSON policy document	1333
Learn more	1333

AWSApplicationDiscoveryAgentlessCollectorAccess	1334
Using this policy	1334
Policy details	1334
Policy version	1334
JSON policy document	1334
Learn more	1335
AWSApplicationDiscoveryServiceFullAccess	1336
Using this policy	1336
Policy details	1336
Policy version	1336
JSON policy document	1336
Learn more	1338
AWSApplicationMigrationAgentInstallationPolicy	1338
Using this policy	1338
Policy details	1338
Policy version	1338
JSON policy document	1339
Learn more	1339
AWSApplicationMigrationAgentPolicy	1340
Using this policy	1340
Policy details	1340
Policy version	1340
JSON policy document	1340
Learn more	1341
AWSApplicationMigrationAgentPolicy_v2	1342
Using this policy	1342
Policy details	1342
Policy version	1342
JSON policy document	1342
Learn more	1343
AWSApplicationMigrationConversionServerPolicy	1343
Using this policy	1343
Policy details	1344
Policy version	1344
JSON policy document	1344
Learn more	1344

AWSApplicationMigrationEC2Access	1345
Using this policy	1345
Policy details	1345
Policy version	1345
JSON policy document	1345
Learn more	1353
AWSApplicationMigrationFullAccess	1353
Using this policy	1353
Policy details	1354
Policy version	1354
JSON policy document	1354
Learn more	1360
AWSApplicationMigrationMGHAccess	1360
Using this policy	1360
Policy details	1360
Policy version	1361
JSON policy document	1361
Learn more	1361
AWSApplicationMigrationReadOnlyAccess	1362
Using this policy	1362
Policy details	1362
Policy version	1362
JSON policy document	1362
Learn more	1363
AWSApplicationMigrationReplicationServerPolicy	1364
Using this policy	1364
Policy details	1364
Policy version	1364
JSON policy document	1364
Learn more	1366
AWSApplicationMigrationServiceEc2InstancePolicy	1366
Using this policy	1367
Policy details	1367
Policy version	1367
JSON policy document	1367
Learn more	1368

AWSApplicationMigrationServiceRolePolicy	1368
Using this policy	1369
Policy details	1369
Policy version	1369
JSON policy document	1369
Learn more	1376
AWSApplicationMigrationSSMAccess	1376
Using this policy	1376
Policy details	1377
Policy version	1377
JSON policy document	1377
Learn more	1379
AWSApplicationMigrationVCenterClientPolicy	1379
Using this policy	1379
Policy details	1379
Policy version	1380
JSON policy document	1380
Learn more	1380
AWSAppMeshEnvoyAccess	1381
Using this policy	1381
Policy details	1381
Policy version	1381
JSON policy document	1381
Learn more	1382
AWSAppMeshFullAccess	1382
Using this policy	1382
Policy details	1382
Policy version	1382
JSON policy document	1383
Learn more	1384
AWSAppMeshPreviewEnvoyAccess	1384
Using this policy	1384
Policy details	1384
Policy version	1385
JSON policy document	1385
Learn more	1385

AWSAppMeshPreviewServiceRolePolicy	1385
Using this policy	1386
Policy details	1386
Policy version	1386
JSON policy document	1386
Learn more	1387
AWSAppMeshReadOnly	1387
Using this policy	1387
Policy details	1387
Policy version	1387
JSON policy document	1387
Learn more	1388
AWSAppMeshServiceRolePolicy	1389
Using this policy	1389
Policy details	1389
Policy version	1389
JSON policy document	1389
Learn more	1390
AWSAppRunnerFullAccess	1390
Using this policy	1390
Policy details	1390
Policy version	1391
JSON policy document	1391
Learn more	1392
AWSAppRunnerReadOnlyAccess	1392
Using this policy	1392
Policy details	1392
Policy version	1392
JSON policy document	1392
Learn more	1393
AWSAppRunnerServicePolicyForECRAccess	1393
Using this policy	1393
Policy details	1393
Policy version	1394
JSON policy document	1394
Learn more	1394

AWSAppSyncAdministrator	1394
Using this policy	1395
Policy details	1395
Policy version	1395
JSON policy document	1395
Learn more	1396
AWSAppSyncInvokeFullAccess	1396
Using this policy	1397
Policy details	1397
Policy version	1397
JSON policy document	1397
Learn more	1398
AWSAppSyncPushToCloudWatchLogs	1398
Using this policy	1398
Policy details	1398
Policy version	1398
JSON policy document	1398
Learn more	1399
AWSAppSyncSchemaAuthor	1399
Using this policy	1399
Policy details	1399
Policy version	1399
JSON policy document	1400
Learn more	1401
AWSAppSyncServiceRolePolicy	1401
Using this policy	1401
Policy details	1401
Policy version	1401
JSON policy document	1402
Learn more	1402
AWSArtifactAccountSync	1402
Using this policy	1402
Policy details	1402
Policy version	1403
JSON policy document	1403
Learn more	1403

AWSArtifactReportsReadOnlyAccess	1403
Using this policy	1404
Policy details	1404
Policy version	1404
JSON policy document	1404
Learn more	1405
AWSArtifactServiceRolePolicy	1405
Using this policy	1405
Policy details	1405
Policy version	1405
JSON policy document	1406
Learn more	1406
AWSAuditManagerAdministratorAccess	1406
Using this policy	1406
Policy details	1406
Policy version	1407
JSON policy document	1407
Learn more	1411
AWSAuditManagerServiceRolePolicy	1411
Using this policy	1411
Policy details	1411
Policy version	1412
JSON policy document	1412
Learn more	1418
AWSAutoScalingPlansEC2AutoScalingPolicy	1419
Using this policy	1419
Policy details	1419
Policy version	1419
JSON policy document	1419
Learn more	1420
AWSBackupAuditAccess	1420
Using this policy	1420
Policy details	1420
Policy version	1420
JSON policy document	1421
Learn more	1422

AWSBackupDataTransferAccess	1422
Using this policy	1422
Policy details	1422
Policy version	1423
JSON policy document	1423
Learn more	1423
AWSBackupFullAccess	1424
Using this policy	1424
Policy details	1424
Policy version	1424
JSON policy document	1424
Learn more	1434
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	1434
Using this policy	1434
Policy details	1434
Policy version	1435
JSON policy document	1435
Learn more	1436
AWSBackupOperatorAccess	1436
Using this policy	1436
Policy details	1436
Policy version	1436
JSON policy document	1436
Learn more	1443
AWSBackupOrganizationAdminAccess	1443
Using this policy	1444
Policy details	1444
Policy version	1444
JSON policy document	1444
Learn more	1446
AWSBackupRestoreAccessForSAPHANA	1446
Using this policy	1446
Policy details	1446
Policy version	1447
JSON policy document	1447
Learn more	1448

AWSBackupServiceLinkedRolePolicyForBackup	1448
Using this policy	1448
Policy details	1448
Policy version	1448
JSON policy document	1449
Learn more	1456
AWSBackupServiceLinkedRolePolicyForBackupTest	1457
Using this policy	1457
Policy details	1457
Policy version	1457
JSON policy document	1457
Learn more	1458
AWSBackupServiceRolePolicyForBackup	1458
Using this policy	1458
Policy details	1458
Policy version	1459
JSON policy document	1459
Learn more	1470
AWSBackupServiceRolePolicyForRestores	1470
Using this policy	1470
Policy details	1470
Policy version	1471
JSON policy document	1471
Learn more	1481
AWSBackupServiceRolePolicyForS3Backup	1481
Using this policy	1481
Policy details	1481
Policy version	1481
JSON policy document	1481
Learn more	1484
AWSBackupServiceRolePolicyForS3Restore	1484
Using this policy	1484
Policy details	1484
Policy version	1484
JSON policy document	1485
Learn more	1486

AWSBatchFullAccess	1486
Using this policy	1486
Policy details	1486
Policy version	1487
JSON policy document	1487
Learn more	1488
AWSBatchServiceEventTargetRole	1488
Using this policy	1489
Policy details	1489
Policy version	1489
JSON policy document	1489
Learn more	1489
AWSBatchServiceRole	1490
Using this policy	1490
Policy details	1490
Policy version	1490
JSON policy document	1490
Learn more	1493
AWSBCMDDataExportsServiceRolePolicy	1494
Using this policy	1494
Policy details	1494
Policy version	1494
JSON policy document	1494
Learn more	1495
AWSBillingConductorFullAccess	1495
Using this policy	1495
Policy details	1495
Policy version	1495
JSON policy document	1496
Learn more	1496
AWSBillingConductorReadOnlyAccess	1496
Using this policy	1496
Policy details	1497
Policy version	1497
JSON policy document	1497
Learn more	1497

AWSBillingReadOnlyAccess	1498
Using this policy	1498
Policy details	1498
Policy version	1498
JSON policy document	1498
Learn more	1500
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	1500
Using this policy	1500
Policy details	1500
Policy version	1500
JSON policy document	1501
Learn more	1502
AWSBudgetsActionsWithAWSResourceControlAccess	1502
Using this policy	1502
Policy details	1502
Policy version	1502
JSON policy document	1502
Learn more	1504
AWSBudgetsReadOnlyAccess	1504
Using this policy	1504
Policy details	1504
Policy version	1504
JSON policy document	1505
Learn more	1505
AWSBugBustFullAccess	1505
Using this policy	1505
Policy details	1505
Policy version	1506
JSON policy document	1506
Learn more	1507
AWSBugBustPlayerAccess	1507
Using this policy	1507
Policy details	1507
Policy version	1508
JSON policy document	1508
Learn more	1509

AWSBugBustServiceRolePolicy	1509
Using this policy	1509
Policy details	1509
Policy version	1510
JSON policy document	1510
Learn more	1510
AWSCertificateManagerFullAccess	1510
Using this policy	1511
Policy details	1511
Policy version	1511
JSON policy document	1511
Learn more	1512
AWSCertificateManagerPrivateCAAuditor	1512
Using this policy	1512
Policy details	1512
Policy version	1513
JSON policy document	1513
Learn more	1513
AWSCertificateManagerPrivateCAFullAccess	1514
Using this policy	1514
Policy details	1514
Policy version	1514
JSON policy document	1514
Learn more	1515
AWSCertificateManagerPrivateCAPrivilegedUser	1515
Using this policy	1515
Policy details	1515
Policy version	1515
JSON policy document	1516
Learn more	1517
AWSCertificateManagerPrivateCAReadOnly	1517
Using this policy	1517
Policy details	1517
Policy version	1518
JSON policy document	1518
Learn more	1518

AWSCertificateManagerPrivateCAUser	1519
Using this policy	1519
Policy details	1519
Policy version	1519
JSON policy document	1519
Learn more	1520
AWSCertificateManagerReadOnly	1521
Using this policy	1521
Policy details	1521
Policy version	1521
JSON policy document	1521
Learn more	1522
AWSChatbotServiceLinkedRolePolicy	1522
Using this policy	1522
Policy details	1522
Policy version	1522
JSON policy document	1523
Learn more	1523
AWSCleanRoomsFullAccess	1524
Using this policy	1524
Policy details	1524
Policy version	1524
JSON policy document	1524
Learn more	1529
AWSCleanRoomsFullAccessNoQuerying	1529
Using this policy	1529
Policy details	1529
Policy version	1529
JSON policy document	1530
Learn more	1534
AWSCleanRoomsMLFullAccess	1535
Using this policy	1535
Policy details	1535
Policy version	1535
JSON policy document	1535
Learn more	1539

AWSCleanRoomsMLReadOnlyAccess	1539
Using this policy	1539
Policy details	1539
Policy version	1539
JSON policy document	1540
Learn more	1541
AWSCleanRoomsReadOnlyAccess	1541
Using this policy	1541
Policy details	1541
Policy version	1541
JSON policy document	1541
Learn more	1543
AWSCloud9Administrator	1543
Using this policy	1543
Policy details	1543
Policy version	1543
JSON policy document	1543
Learn more	1545
AWSCloud9EnvironmentMember	1545
Using this policy	1545
Policy details	1545
Policy version	1545
JSON policy document	1546
Learn more	1547
AWSCloud9ServiceRolePolicy	1547
Using this policy	1547
Policy details	1547
Policy version	1548
JSON policy document	1548
Learn more	1550
AWSCloud9SSMInstanceProfile	1550
Using this policy	1551
Policy details	1551
Policy version	1551
JSON policy document	1551
Learn more	1552

AWSCloud9User	1552
Using this policy	1552
Policy details	1552
Policy version	1552
JSON policy document	1552
Learn more	1555
AWSCloudFormationFullAccess	1555
Using this policy	1555
Policy details	1555
Policy version	1555
JSON policy document	1556
Learn more	1556
AWSCloudFormationReadOnlyAccess	1556
Using this policy	1556
Policy details	1556
Policy version	1557
JSON policy document	1557
Learn more	1557
AWSCloudFrontLogger	1557
Using this policy	1558
Policy details	1558
Policy version	1558
JSON policy document	1558
Learn more	1559
AWSCloudHSMFullAccess	1559
Using this policy	1559
Policy details	1559
Policy version	1559
JSON policy document	1559
Learn more	1560
AWSCloudHSMReadOnlyAccess	1560
Using this policy	1560
Policy details	1560
Policy version	1560
JSON policy document	1561
Learn more	1561

AWSCloudHSMRole	1561
Using this policy	1561
Policy details	1561
Policy version	1562
JSON policy document	1562
Learn more	1562
AWSCloudMapDiscoverInstanceAccess	1563
Using this policy	1563
Policy details	1563
Policy version	1563
JSON policy document	1563
Learn more	1564
AWSCloudMapFullAccess	1564
Using this policy	1564
Policy details	1564
Policy version	1564
JSON policy document	1565
Learn more	1565
AWSCloudMapReadOnlyAccess	1565
Using this policy	1566
Policy details	1566
Policy version	1566
JSON policy document	1566
Learn more	1567
AWSCloudMapRegisterInstanceAccess	1567
Using this policy	1567
Policy details	1567
Policy version	1567
JSON policy document	1567
Learn more	1568
AWSCloudShellFullAccess	1568
Using this policy	1568
Policy details	1569
Policy version	1569
JSON policy document	1569
Learn more	1569

AWSCloudTrail_FullAccess	1570
Using this policy	1570
Policy details	1570
Policy version	1570
JSON policy document	1570
Learn more	1573
AWSCloudTrail_ReadOnlyAccess	1573
Using this policy	1573
Policy details	1573
Policy version	1573
JSON policy document	1574
Learn more	1574
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	1574
Using this policy	1574
Policy details	1575
Policy version	1575
JSON policy document	1575
Learn more	1575
AWSCodeArtifactAdminAccess	1575
Using this policy	1576
Policy details	1576
Policy version	1576
JSON policy document	1576
Learn more	1577
AWSCodeArtifactReadOnlyAccess	1577
Using this policy	1577
Policy details	1577
Policy version	1577
JSON policy document	1578
Learn more	1578
AWSCodeBuildAdminAccess	1579
Using this policy	1579
Policy details	1579
Policy version	1579
JSON policy document	1579
Learn more	1583

AWSCodeBuildDeveloperAccess	1583
Using this policy	1583
Policy details	1583
Policy version	1583
JSON policy document	1583
Learn more	1586
AWSCodeBuildReadOnlyAccess	1586
Using this policy	1586
Policy details	1587
Policy version	1587
JSON policy document	1587
Learn more	1588
AWSCodeCommitFullAccess	1589
Using this policy	1589
Policy details	1589
Policy version	1589
JSON policy document	1589
Learn more	1594
AWSCodeCommitPowerUser	1594
Using this policy	1594
Policy details	1594
Policy version	1595
JSON policy document	1595
Learn more	1599
AWSCodeCommitReadOnly	1600
Using this policy	1600
Policy details	1600
Policy version	1600
JSON policy document	1600
Learn more	1603
AWSCodeDeployDeployerAccess	1603
Using this policy	1603
Policy details	1603
Policy version	1604
JSON policy document	1604
Learn more	1605

AWSCodeDeployFullAccess	1605
Using this policy	1606
Policy details	1606
Policy version	1606
JSON policy document	1606
Learn more	1608
AWSCodeDeployReadOnlyAccess	1608
Using this policy	1608
Policy details	1608
Policy version	1608
JSON policy document	1608
Learn more	1609
AWSCodeDeployRole	1610
Using this policy	1610
Policy details	1610
Policy version	1610
JSON policy document	1610
Learn more	1612
AWSCodeDeployRoleForCloudFormation	1612
Using this policy	1612
Policy details	1612
Policy version	1612
JSON policy document	1612
Learn more	1613
AWSCodeDeployRoleForECS	1613
Using this policy	1613
Policy details	1613
Policy version	1614
JSON policy document	1614
Learn more	1615
AWSCodeDeployRoleForECSLimited	1615
Using this policy	1615
Policy details	1615
Policy version	1615
JSON policy document	1616
Learn more	1617

AWSCodeDeployRoleForLambda	1618
Using this policy	1618
Policy details	1618
Policy version	1618
JSON policy document	1618
Learn more	1619
AWSCodeDeployRoleForLambdaLimited	1620
Using this policy	1620
Policy details	1620
Policy version	1620
JSON policy document	1620
Learn more	1621
AWSCodePipeline_FullAccess	1622
Using this policy	1622
Policy details	1622
Policy version	1622
JSON policy document	1622
Learn more	1626
AWSCodePipeline_ReadOnlyAccess	1626
Using this policy	1626
Policy details	1626
Policy version	1627
JSON policy document	1627
Learn more	1628
AWSCodePipelineApproverAccess	1628
Using this policy	1628
Policy details	1628
Policy version	1629
JSON policy document	1629
Learn more	1629
AWSCodePipelineCustomActionAccess	1629
Using this policy	1630
Policy details	1630
Policy version	1630
JSON policy document	1630
Learn more	1631

AWSCodeStarFullAccess	1631
Using this policy	1631
Policy details	1631
Policy version	1631
JSON policy document	1631
Learn more	1632
AWSCodeStarNotificationsServiceRolePolicy	1632
Using this policy	1633
Policy details	1633
Policy version	1633
JSON policy document	1633
Learn more	1634
AWSCodeStarServiceRole	1634
Using this policy	1635
Policy details	1635
Policy version	1635
JSON policy document	1635
Learn more	1640
AWSCompromisedKeyQuarantine	1640
Using this policy	1640
Policy details	1640
Policy version	1641
JSON policy document	1641
Learn more	1642
AWSCompromisedKeyQuarantineV2	1642
Using this policy	1642
Policy details	1642
Policy version	1642
JSON policy document	1643
Learn more	1644
AWSConfigMultiAccountSetupPolicy	1645
Using this policy	1645
Policy details	1645
Policy version	1645
JSON policy document	1645
Learn more	1647

AWSServiceRolePolicy	1647
Using this policy	1648
Policy details	1648
Policy version	1648
JSON policy document	1648
Learn more	1649
AWSServiceRolePolicyForOrganizations	1649
Using this policy	1649
Policy details	1649
Policy version	1649
JSON policy document	1650
Learn more	1650
AWSServiceRolePolicyForDelegatedAdmins	1650
Using this policy	1650
Policy details	1651
Policy version	1651
JSON policy document	1651
Learn more	1652
AWSServiceRolePolicyForLambda	1652
Using this policy	1652
Policy details	1652
Policy version	1652
JSON policy document	1653
Learn more	1684
AWSServiceRolePolicyForECS	1684
Using this policy	1684
Policy details	1684
Policy version	1685
JSON policy document	1685
Learn more	1685
AWSServiceRolePolicyForEKS	1686
Using this policy	1686
Policy details	1686
Policy version	1686
JSON policy document	1686
Learn more	1688

AWSControlTowerAccountServiceRolePolicy	1689
Using this policy	1689
Policy details	1689
Policy version	1689
JSON policy document	1689
Learn more	1691
AWSControlTowerServiceRolePolicy	1691
Using this policy	1691
Policy details	1691
Policy version	1692
JSON policy document	1692
Learn more	1696
AWSCostAndUsageReportAutomationPolicy	1696
Using this policy	1697
Policy details	1697
Policy version	1697
JSON policy document	1697
Learn more	1698
AWSDataExchangeFullAccess	1698
Using this policy	1698
Policy details	1699
Policy version	1699
JSON policy document	1699
Learn more	1702
AWSDataExchangeProviderFullAccess	1703
Using this policy	1703
Policy details	1703
Policy version	1703
JSON policy document	1703
Learn more	1707
AWSDataExchangeReadOnly	1707
Using this policy	1707
Policy details	1707
Policy version	1707
JSON policy document	1708
Learn more	1708

AWSDataExchangeSubscriberFullAccess	1709
Using this policy	1709
Policy details	1709
Policy version	1709
JSON policy document	1709
Learn more	1712
AWSDataLifecycleManagerServiceRole	1712
Using this policy	1712
Policy details	1712
Policy version	1712
JSON policy document	1712
Learn more	1714
AWSDataLifecycleManagerServiceRoleForAMIManagement	1714
Using this policy	1714
Policy details	1714
Policy version	1714
JSON policy document	1715
Learn more	1716
AWSDataLifecycleManagerSSMFullAccess	1716
Using this policy	1716
Policy details	1716
Policy version	1716
JSON policy document	1717
Learn more	1718
AWSDataPipeline_FullAccess	1718
Using this policy	1718
Policy details	1718
Policy version	1719
JSON policy document	1719
Learn more	1720
AWSDataPipeline_PowerUser	1720
Using this policy	1720
Policy details	1720
Policy version	1720
JSON policy document	1721
Learn more	1722

AWSDataSyncDiscoveryServiceRolePolicy	1722
Using this policy	1722
Policy details	1722
Policy version	1722
JSON policy document	1722
Learn more	1723
AWSDataSyncFullAccess	1724
Using this policy	1724
Policy details	1724
Policy version	1724
JSON policy document	1724
Learn more	1726
AWSDataSyncReadOnlyAccess	1726
Using this policy	1726
Policy details	1726
Policy version	1726
JSON policy document	1726
Learn more	1727
AWSDeadlineCloud-FleetWorker	1727
Using this policy	1727
Policy details	1728
Policy version	1728
JSON policy document	1728
Learn more	1729
AWSDeadlineCloud-UserAccessFarms	1729
Using this policy	1729
Policy details	1729
Policy version	1729
JSON policy document	1729
Learn more	1735
AWSDeadlineCloud-UserAccessFleets	1735
Using this policy	1735
Policy details	1735
Policy version	1735
JSON policy document	1736
Learn more	1739

AWSDeadlineCloud-UserAccessJobs	1740
Using this policy	1740
Policy details	1740
Policy version	1740
JSON policy document	1740
Learn more	1744
AWSDeadlineCloud-UserAccessQueues	1744
Using this policy	1744
Policy details	1745
Policy version	1745
JSON policy document	1745
Learn more	1750
AWSDeadlineCloud-WorkerHost	1750
Using this policy	1750
Policy details	1750
Policy version	1750
JSON policy document	1750
Learn more	1751
AWSDeepLensLambdaFunctionAccessPolicy	1751
Using this policy	1751
Policy details	1751
Policy version	1752
JSON policy document	1752
Learn more	1753
AWSDeepLensServiceRolePolicy	1753
Using this policy	1753
Policy details	1754
Policy version	1754
JSON policy document	1754
Learn more	1761
AWSDeepRacerAccountAdminAccess	1761
Using this policy	1761
Policy details	1761
Policy version	1762
JSON policy document	1762
Learn more	1762

AWSDepRacerCloudFormationAccessPolicy	1763
Using this policy	1763
Policy details	1763
Policy version	1763
JSON policy document	1763
Learn more	1766
AWSDepRacerDefaultMultiUserAccess	1766
Using this policy	1767
Policy details	1767
Policy version	1767
JSON policy document	1767
Learn more	1768
AWSDepRacerFullAccess	1769
Using this policy	1769
Policy details	1769
Policy version	1769
JSON policy document	1769
Learn more	1770
AWSDepRacerRoboMakerAccessPolicy	1771
Using this policy	1771
Policy details	1771
Policy version	1771
JSON policy document	1771
Learn more	1773
AWSDepRacerServiceRolePolicy	1773
Using this policy	1773
Policy details	1774
Policy version	1774
JSON policy document	1774
Learn more	1777
AWSDenyAll	1777
Using this policy	1777
Policy details	1778
Policy version	1778
JSON policy document	1778
Learn more	1778

AWSDirectoryServiceFullAccess	1790
Using this policy	1790
Policy details	1790
Policy version	1790
JSON policy document	1790
Learn more	1792
AWSDirectoryServiceReadOnlyAccess	1792
Using this policy	1793
Policy details	1793
Policy version	1793
JSON policy document	1793
Learn more	1794
AWSDiscoveryContinuousExportFirehosePolicy	1794
Using this policy	1794
Policy details	1794
Policy version	1794
JSON policy document	1795
Learn more	1796
AWSDMSFleetAdvisorServiceRolePolicy	1796
Using this policy	1796
Policy details	1796
Policy version	1796
JSON policy document	1796
Learn more	1797
AWSDMSServerlessServiceRolePolicy	1797
Using this policy	1797
Policy details	1797
Policy version	1798
JSON policy document	1798
Learn more	1799
AWSEC2CapacityReservationFleetRolePolicy	1799
Using this policy	1800
Policy details	1800
Policy version	1800
JSON policy document	1800
Learn more	1801

AWSEC2FleetServiceRolePolicy	1801
Using this policy	1802
Policy details	1802
Policy version	1802
JSON policy document	1802
Learn more	1804
AWSEC2SpotFleetServiceRolePolicy	1804
Using this policy	1804
Policy details	1805
Policy version	1805
JSON policy document	1805
Learn more	1807
AWSEC2SpotServiceRolePolicy	1807
Using this policy	1807
Policy details	1807
Policy version	1807
JSON policy document	1808
Learn more	1809
AWSEC2VssSnapshotPolicy	1809
Using this policy	1809
Policy details	1810
Policy version	1810
JSON policy document	1810
Learn more	1813
AWSECRPullThroughCache_ServiceRolePolicy	1813
Using this policy	1814
Policy details	1814
Policy version	1814
JSON policy document	1814
Learn more	1815
AWSElasticBeanstalkCustomPlatformforEC2Role	1815
Using this policy	1815
Policy details	1815
Policy version	1816
JSON policy document	1816
Learn more	1817

AWSElasticBeanstalkEnhancedHealth	1818
Using this policy	1818
Policy details	1818
Policy version	1818
JSON policy document	1818
Learn more	1819
AWSElasticBeanstalkMaintenance	1819
Using this policy	1820
Policy details	1820
Policy version	1820
JSON policy document	1820
Learn more	1821
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	1821
Using this policy	1821
Policy details	1821
Policy version	1822
JSON policy document	1822
Learn more	1828
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	1829
Using this policy	1829
Policy details	1829
Policy version	1829
JSON policy document	1829
Learn more	1835
AWSElasticBeanstalkMulticontainerDocker	1835
Using this policy	1835
Policy details	1835
Policy version	1835
JSON policy document	1836
Learn more	1837
AWSElasticBeanstalkReadOnly	1837
Using this policy	1837
Policy details	1837
Policy version	1837
JSON policy document	1837
Learn more	1840

AWSElasticBeanstalkRoleCore	1840
Using this policy	1840
Policy details	1840
Policy version	1840
JSON policy document	1840
Learn more	1845
AWSElasticBeanstalkRoleCWL	1846
Using this policy	1846
Policy details	1846
Policy version	1846
JSON policy document	1846
Learn more	1847
AWSElasticBeanstalkRoleECS	1847
Using this policy	1847
Policy details	1847
Policy version	1847
JSON policy document	1848
Learn more	1848
AWSElasticBeanstalkRoleRDS	1849
Using this policy	1849
Policy details	1849
Policy version	1849
JSON policy document	1849
Learn more	1850
AWSElasticBeanstalkRoleSNS	1850
Using this policy	1850
Policy details	1850
Policy version	1851
JSON policy document	1851
Learn more	1851
AWSElasticBeanstalkRoleWorkerTier	1852
Using this policy	1852
Policy details	1852
Policy version	1852
JSON policy document	1852
Learn more	1853

AWSElasticBeanstalkService	1853
Using this policy	1854
Policy details	1854
Policy version	1854
JSON policy document	1854
Learn more	1858
AWSElasticBeanstalkServiceRolePolicy	1859
Using this policy	1859
Policy details	1859
Policy version	1859
JSON policy document	1859
Learn more	1861
AWSElasticBeanstalkWebTier	1861
Using this policy	1861
Policy details	1861
Policy version	1861
JSON policy document	1862
Learn more	1863
AWSElasticBeanstalkWorkerTier	1863
Using this policy	1863
Policy details	1863
Policy version	1864
JSON policy document	1864
Learn more	1866
AWSElasticDisasterRecoveryAgentInstallationPolicy	1866
Using this policy	1866
Policy details	1866
Policy version	1867
JSON policy document	1867
Learn more	1868
AWSElasticDisasterRecoveryAgentPolicy	1869
Using this policy	1869
Policy details	1869
Policy version	1869
JSON policy document	1869
Learn more	1870

AWSElasticDisasterRecoveryConsoleFullAccess	1870
Using this policy	1871
Policy details	1871
Policy version	1871
JSON policy document	1871
Learn more	1881
AWSElasticDisasterRecoveryConsoleFullAccess_v2	1881
Using this policy	1881
Policy details	1881
Policy version	1882
JSON policy document	1882
Learn more	1894
AWSElasticDisasterRecoveryConversionServerPolicy	1895
Using this policy	1895
Policy details	1895
Policy version	1895
JSON policy document	1895
Learn more	1896
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	1896
Using this policy	1896
Policy details	1897
Policy version	1897
JSON policy document	1897
Learn more	1898
AWSElasticDisasterRecoveryEc2InstancePolicy	1898
Using this policy	1898
Policy details	1898
Policy version	1899
JSON policy document	1899
Learn more	1901
AWSElasticDisasterRecoveryFailbackInstallationPolicy	1901
Using this policy	1901
Policy details	1901
Policy version	1901
JSON policy document	1902
Learn more	1902

AWSElasticDisasterRecoveryFailbackPolicy	1903
Using this policy	1903
Policy details	1903
Policy version	1903
JSON policy document	1903
Learn more	1905
AWSElasticDisasterRecoveryLaunchActionsPolicy	1905
Using this policy	1905
Policy details	1905
Policy version	1905
JSON policy document	1906
Learn more	1911
AWSElasticDisasterRecoveryNetworkReplicationPolicy	1912
Using this policy	1912
Policy details	1912
Policy version	1912
JSON policy document	1912
Learn more	1913
AWSElasticDisasterRecoveryReadOnlyAccess	1913
Using this policy	1914
Policy details	1914
Policy version	1914
JSON policy document	1914
Learn more	1916
AWSElasticDisasterRecoveryRecoveryInstancePolicy	1916
Using this policy	1917
Policy details	1917
Policy version	1917
JSON policy document	1917
Learn more	1920
AWSElasticDisasterRecoveryReplicationServerPolicy	1920
Using this policy	1920
Policy details	1920
Policy version	1921
JSON policy document	1921
Learn more	1923

AWSElasticDisasterRecoveryServiceRolePolicy	1923
Using this policy	1923
Policy details	1923
Policy version	1924
JSON policy document	1924
Learn more	1932
AWSElasticDisasterRecoveryStagingAccountPolicy	1932
Using this policy	1933
Policy details	1933
Policy version	1933
JSON policy document	1933
Learn more	1934
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	1934
Using this policy	1934
Policy details	1935
Policy version	1935
JSON policy document	1935
Learn more	1936
AWSElasticLoadBalancingClassicServiceRolePolicy	1936
Using this policy	1936
Policy details	1937
Policy version	1937
JSON policy document	1937
Learn more	1938
AWSElasticLoadBalancingServiceRolePolicy	1938
Using this policy	1938
Policy details	1938
Policy version	1938
JSON policy document	1939
Learn more	1940
AWSElementalMediaConvertFullAccess	1940
Using this policy	1940
Policy details	1940
Policy version	1940
JSON policy document	1941
Learn more	1941

AWSElementalMediaConvertReadOnly	1942
Using this policy	1942
Policy details	1942
Policy version	1942
JSON policy document	1942
Learn more	1943
AWSElementalMediaLiveFullAccess	1943
Using this policy	1943
Policy details	1943
Policy version	1943
JSON policy document	1944
Learn more	1944
AWSElementalMediaLiveReadOnly	1944
Using this policy	1944
Policy details	1944
Policy version	1945
JSON policy document	1945
Learn more	1945
AWSElementalMediaPackageFullAccess	1945
Using this policy	1945
Policy details	1946
Policy version	1946
JSON policy document	1946
Learn more	1946
AWSElementalMediaPackageReadOnly	1946
Using this policy	1947
Policy details	1947
Policy version	1947
JSON policy document	1947
Learn more	1947
AWSElementalMediaPackageV2FullAccess	1948
Using this policy	1948
Policy details	1948
Policy version	1948
JSON policy document	1948
Learn more	1949

AWSElementalMediaPackageV2ReadOnly	1949
Using this policy	1949
Policy details	1949
Policy version	1949
JSON policy document	1949
Learn more	1950
AWSElementalMediaStoreFullAccess	1950
Using this policy	1950
Policy details	1950
Policy version	1950
JSON policy document	1951
Learn more	1951
AWSElementalMediaStoreReadOnly	1951
Using this policy	1951
Policy details	1952
Policy version	1952
JSON policy document	1952
Learn more	1952
AWSElementalMediaTailorFullAccess	1953
Using this policy	1953
Policy details	1953
Policy version	1953
JSON policy document	1953
Learn more	1954
AWSElementalMediaTailorReadOnly	1954
Using this policy	1954
Policy details	1954
Policy version	1954
JSON policy document	1954
Learn more	1955
AWSEnhancedClassicNetworkingMangementPolicy	1955
Using this policy	1955
Policy details	1955
Policy version	1956
JSON policy document	1956
Learn more	1956

AWSEntityResolutionConsoleFullAccess	1956
Using this policy	1956
Policy details	1957
Policy version	1957
JSON policy document	1957
Learn more	1960
AWSEntityResolutionConsoleReadOnlyAccess	1960
Using this policy	1960
Policy details	1960
Policy version	1960
JSON policy document	1961
Learn more	1961
AWSFaultInjectionSimulatorEC2Access	1961
Using this policy	1961
Policy details	1961
Policy version	1962
JSON policy document	1962
Learn more	1963
AWSFaultInjectionSimulatorECSAccess	1964
Using this policy	1964
Policy details	1964
Policy version	1964
JSON policy document	1964
Learn more	1966
AWSFaultInjectionSimulatorEKSAccess	1966
Using this policy	1966
Policy details	1966
Policy version	1967
JSON policy document	1967
Learn more	1968
AWSFaultInjectionSimulatorNetworkAccess	1968
Using this policy	1968
Policy details	1968
Policy version	1969
JSON policy document	1969
Learn more	1976

AWSFaultInjectionSimulatorRDSAccess	1976
Using this policy	1976
Policy details	1976
Policy version	1976
JSON policy document	1977
Learn more	1978
AWSFaultInjectionSimulatorSSMAccess	1978
Using this policy	1978
Policy details	1978
Policy version	1978
JSON policy document	1979
Learn more	1980
AWSFinSpaceServiceRolePolicy	1980
Using this policy	1980
Policy details	1980
Policy version	1981
JSON policy document	1981
Learn more	1981
AWSFMAdminFullAccess	1981
Using this policy	1982
Policy details	1982
Policy version	1982
JSON policy document	1982
Learn more	1984
AWSFMAdminReadOnlyAccess	1984
Using this policy	1984
Policy details	1984
Policy version	1985
JSON policy document	1985
Learn more	1986
AWSFMMemberReadOnlyAccess	1986
Using this policy	1987
Policy details	1987
Policy version	1987
JSON policy document	1987
Learn more	1988

AWSForWordPressPluginPolicy	1988
Using this policy	1988
Policy details	1988
Policy version	1988
JSON policy document	1988
Learn more	1990
AWSGitSyncServiceRolePolicy	1990
Using this policy	1991
Policy details	1991
Policy version	1991
JSON policy document	1991
Learn more	1992
AWSGlobalAcceleratorSLRPolicy	1992
Using this policy	1992
Policy details	1992
Policy version	1992
JSON policy document	1993
Learn more	1994
AWSGlueConsoleFullAccess	1994
Using this policy	1994
Policy details	1995
Policy version	1995
JSON policy document	1995
Learn more	1999
AWSGlueConsoleSageMakerNotebookFullAccess	1999
Using this policy	2000
Policy details	2000
Policy version	2000
JSON policy document	2000
Learn more	2005
AwsGlueDataBrewFullAccessPolicy	2005
Using this policy	2006
Policy details	2006
Policy version	2006
JSON policy document	2006
Learn more	2011

AWSGlueDataBrewServiceRole	2011
Using this policy	2012
Policy details	2012
Policy version	2012
JSON policy document	2012
Learn more	2015
AWSGlueSchemaRegistryFullAccess	2015
Using this policy	2015
Policy details	2015
Policy version	2016
JSON policy document	2016
Learn more	2017
AWSGlueSchemaRegistryReadOnlyAccess	2017
Using this policy	2017
Policy details	2017
Policy version	2018
JSON policy document	2018
Learn more	2018
AWSGlueServiceNotebookRole	2019
Using this policy	2019
Policy details	2019
Policy version	2019
JSON policy document	2019
Learn more	2022
AWSGlueServiceRole	2022
Using this policy	2022
Policy details	2022
Policy version	2022
JSON policy document	2022
Learn more	2025
AwsGlueSessionUserRestrictedNotebookPolicy	2025
Using this policy	2025
Policy details	2025
Policy version	2025
JSON policy document	2026
Learn more	2028

AwsGlueSessionUserRestrictedNotebookServiceRole	2028
Using this policy	2028
Policy details	2029
Policy version	2029
JSON policy document	2029
Learn more	2033
AwsGlueSessionUserRestrictedPolicy	2033
Using this policy	2033
Policy details	2033
Policy version	2033
JSON policy document	2033
Learn more	2036
AwsGlueSessionUserRestrictedServiceRole	2036
Using this policy	2036
Policy details	2036
Policy version	2037
JSON policy document	2037
Learn more	2041
AWSGrafanaAccountAdministrator	2041
Using this policy	2041
Policy details	2041
Policy version	2042
JSON policy document	2042
Learn more	2043
AWSGrafanaConsoleReadOnlyAccess	2043
Using this policy	2043
Policy details	2043
Policy version	2043
JSON policy document	2044
Learn more	2044
AWSGrafanaWorkspacePermissionManagement	2044
Using this policy	2044
Policy details	2045
Policy version	2045
JSON policy document	2045
Learn more	2046

AWSGrafanaWorkspacePermissionManagementV2	2046
Using this policy	2046
Policy details	2046
Policy version	2047
JSON policy document	2047
Learn more	2048
AWSGreengrassFullAccess	2048
Using this policy	2048
Policy details	2048
Policy version	2048
JSON policy document	2049
Learn more	2049
AWSGreengrassReadOnlyAccess	2049
Using this policy	2049
Policy details	2049
Policy version	2050
JSON policy document	2050
Learn more	2050
AWSGreengrassResourceAccessRolePolicy	2050
Using this policy	2051
Policy details	2051
Policy version	2051
JSON policy document	2051
Learn more	2053
AWSGroundStationAgentInstancePolicy	2054
Using this policy	2054
Policy details	2054
Policy version	2054
JSON policy document	2054
Learn more	2055
AWSHealth_EventProcessorServiceRolePolicy	2055
Using this policy	2055
Policy details	2055
Policy version	2055
JSON policy document	2056
Learn more	2056

AWSHealthFullAccess	2056
Using this policy	2057
Policy details	2057
Policy version	2057
JSON policy document	2057
Learn more	2058
AWSHealthImagingFullAccess	2058
Using this policy	2058
Policy details	2059
Policy version	2059
JSON policy document	2059
Learn more	2060
AWSHealthImagingReadOnlyAccess	2060
Using this policy	2060
Policy details	2060
Policy version	2060
JSON policy document	2060
Learn more	2061
AWSIAMIdentityCenterAllowListForIdentityContext	2061
Using this policy	2061
Policy details	2062
Policy version	2062
JSON policy document	2062
Learn more	2065
AWSIdentitySyncFullAccess	2065
Using this policy	2065
Policy details	2065
Policy version	2066
JSON policy document	2066
Learn more	2067
AWSIdentitySyncReadOnlyAccess	2067
Using this policy	2067
Policy details	2067
Policy version	2067
JSON policy document	2067
Learn more	2068

AWSImageBuilderFullAccess	2068
Using this policy	2068
Policy details	2068
Policy version	2069
JSON policy document	2069
Learn more	2071
AWSImageBuilderReadOnlyAccess	2072
Using this policy	2072
Policy details	2072
Policy version	2072
JSON policy document	2072
Learn more	2073
AWSImportExportFullAccess	2073
Using this policy	2073
Policy details	2073
Policy version	2073
JSON policy document	2074
Learn more	2074
AWSImportExportReadOnlyAccess	2074
Using this policy	2074
Policy details	2074
Policy version	2075
JSON policy document	2075
Learn more	2075
AWSIncidentManagerIncidentAccessServiceRolePolicy	2076
Using this policy	2076
Policy details	2076
Policy version	2076
JSON policy document	2076
Learn more	2077
AWSIncidentManagerResolverAccess	2077
Using this policy	2077
Policy details	2077
Policy version	2078
JSON policy document	2078
Learn more	2079

AWSIncidentManagerServiceRolePolicy	2079
Using this policy	2079
Policy details	2079
Policy version	2079
JSON policy document	2080
Learn more	2081
AWSIoT1ClickFullAccess	2081
Using this policy	2081
Policy details	2081
Policy version	2081
JSON policy document	2082
Learn more	2082
AWSIoT1ClickReadOnlyAccess	2082
Using this policy	2082
Policy details	2082
Policy version	2083
JSON policy document	2083
Learn more	2083
AWSIoTAnalyticsFullAccess	2083
Using this policy	2084
Policy details	2084
Policy version	2084
JSON policy document	2084
Learn more	2084
AWSIoTAnalyticsReadOnlyAccess	2085
Using this policy	2085
Policy details	2085
Policy version	2085
JSON policy document	2085
Learn more	2086
AWSIoTConfigAccess	2086
Using this policy	2086
Policy details	2086
Policy version	2086
JSON policy document	2087
Learn more	2090

AWSIoTConfigReadOnlyAccess	2091
Using this policy	2091
Policy details	2091
Policy version	2091
JSON policy document	2091
Learn more	2093
AWSIoTDataAccess	2093
Using this policy	2094
Policy details	2094
Policy version	2094
JSON policy document	2094
Learn more	2095
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	2095
Using this policy	2095
Policy details	2095
Policy version	2095
JSON policy document	2096
Learn more	2096
AWSIoTDeviceDefenderAudit	2096
Using this policy	2096
Policy details	2096
Policy version	2097
JSON policy document	2097
Learn more	2098
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	2098
Using this policy	2098
Policy details	2098
Policy version	2098
JSON policy document	2099
Learn more	2099
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	2100
Using this policy	2100
Policy details	2100
Policy version	2100
JSON policy document	2100
Learn more	2101

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	2101
Using this policy	2101
Policy details	2101
Policy version	2102
JSON policy document	2102
Learn more	2102
AWSIoTDeviceDefenderUpdateCACertMitigationAction	2102
Using this policy	2103
Policy details	2103
Policy version	2103
JSON policy document	2103
Learn more	2104
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	2104
Using this policy	2104
Policy details	2104
Policy version	2104
JSON policy document	2105
Learn more	2105
AWSIoTDeviceTesterForFreeRTOSFullAccess	2105
Using this policy	2105
Policy details	2105
Policy version	2106
JSON policy document	2106
Learn more	2112
AWSIoTDeviceTesterForGreengrassFullAccess	2112
Using this policy	2112
Policy details	2112
Policy version	2113
JSON policy document	2113
Learn more	2116
AWSIoTEventsFullAccess	2116
Using this policy	2116
Policy details	2116
Policy version	2116
JSON policy document	2117
Learn more	2117

AWSIoTEventsReadOnlyAccess	2117
Using this policy	2117
Policy details	2117
Policy version	2118
JSON policy document	2118
Learn more	2118
AWSIoTFleetHubFederationAccess	2118
Using this policy	2118
Policy details	2119
Policy version	2119
JSON policy document	2119
Learn more	2121
AWSIoTFleetwiseServiceRolePolicy	2121
Using this policy	2121
Policy details	2121
Policy version	2121
JSON policy document	2122
Learn more	2122
AWSIoTFullAccess	2122
Using this policy	2122
Policy details	2123
Policy version	2123
JSON policy document	2123
Learn more	2123
AWSIoTLogging	2124
Using this policy	2124
Policy details	2124
Policy version	2124
JSON policy document	2124
Learn more	2125
AWSIoTOTAUpdate	2125
Using this policy	2125
Policy details	2125
Policy version	2125
JSON policy document	2126
Learn more	2126

AWSIoTRoboRunnerFullAccess	2126
Using this policy	2126
Policy details	2126
Policy version	2127
JSON policy document	2127
Learn more	2127
AWSIoTRoboRunnerReadOnly	2128
Using this policy	2128
Policy details	2128
Policy version	2128
JSON policy document	2128
Learn more	2129
AWSIoTRoboRunnerServiceRolePolicy	2129
Using this policy	2129
Policy details	2129
Policy version	2130
JSON policy document	2130
Learn more	2130
AWSIoTRuleActions	2130
Using this policy	2131
Policy details	2131
Policy version	2131
JSON policy document	2131
Learn more	2132
AWSIoTSiteWiseConsoleFullAccess	2132
Using this policy	2132
Policy details	2132
Policy version	2132
JSON policy document	2133
Learn more	2135
AWSIoTSiteWiseFullAccess	2135
Using this policy	2135
Policy details	2135
Policy version	2135
JSON policy document	2136
Learn more	2136

AWSIoTSiteWiseMonitorPortalAccess	2136
Using this policy	2136
Policy details	2136
Policy version	2137
JSON policy document	2137
Learn more	2138
AWSIoTSiteWiseMonitorServiceRolePolicy	2138
Using this policy	2138
Policy details	2138
Policy version	2139
JSON policy document	2139
Learn more	2140
AWSIoTSiteWiseReadOnlyAccess	2140
Using this policy	2140
Policy details	2140
Policy version	2140
JSON policy document	2140
Learn more	2141
AWSIoTThingsRegistration	2141
Using this policy	2141
Policy details	2141
Policy version	2142
JSON policy document	2142
Learn more	2143
AWSIoTtwinMakerServiceRolePolicy	2143
Using this policy	2143
Policy details	2143
Policy version	2144
JSON policy document	2144
Learn more	2145
AWSIoTWirelessDataAccess	2145
Using this policy	2146
Policy details	2146
Policy version	2146
JSON policy document	2146
Learn more	2146

AWSIoTWirelessFullAccess	2147
Using this policy	2147
Policy details	2147
Policy version	2147
JSON policy document	2147
Learn more	2148
AWSIoTWirelessFullPublishAccess	2148
Using this policy	2148
Policy details	2148
Policy version	2148
JSON policy document	2149
Learn more	2149
AWSIoTWirelessGatewayCertManager	2149
Using this policy	2149
Policy details	2149
Policy version	2150
JSON policy document	2150
Learn more	2150
AWSIoTWirelessLogging	2151
Using this policy	2151
Policy details	2151
Policy version	2151
JSON policy document	2151
Learn more	2152
AWSIoTWirelessReadOnlyAccess	2152
Using this policy	2152
Policy details	2152
Policy version	2152
JSON policy document	2153
Learn more	2153
AWSIPAMServiceRolePolicy	2153
Using this policy	2153
Policy details	2153
Policy version	2154
JSON policy document	2154
Learn more	2155

AWSIQContractServiceRolePolicy	2155
Using this policy	2155
Policy details	2155
Policy version	2156
JSON policy document	2156
Learn more	2156
AWSIQFullAccess	2156
Using this policy	2156
Policy details	2157
Policy version	2157
JSON policy document	2157
Learn more	2158
AWSIQPermissionServiceRolePolicy	2158
Using this policy	2158
Policy details	2158
Policy version	2158
JSON policy document	2159
Learn more	2159
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2160
Using this policy	2160
Policy details	2160
Policy version	2160
JSON policy document	2160
Learn more	2161
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2161
Using this policy	2161
Policy details	2161
Policy version	2162
JSON policy document	2162
Learn more	2162
AWSKeyManagementServicePowerUser	2162
Using this policy	2162
Policy details	2163
Policy version	2163
JSON policy document	2163
Learn more	2164

AWSLakeFormationCrossAccountManager	2164
Using this policy	2164
Policy details	2164
Policy version	2164
JSON policy document	2164
Learn more	2166
AWSLakeFormationDataAdmin	2167
Using this policy	2167
Policy details	2167
Policy version	2167
JSON policy document	2167
Learn more	2168
AWSLambda_FullAccess	2169
Using this policy	2169
Policy details	2169
Policy version	2169
JSON policy document	2169
Learn more	2171
AWSLambda_ReadOnlyAccess	2171
Using this policy	2171
Policy details	2171
Policy version	2171
JSON policy document	2172
Learn more	2173
AWSLambdaBasicExecutionRole	2173
Using this policy	2173
Policy details	2173
Policy version	2173
JSON policy document	2174
Learn more	2174
AWSLambdaDynamoDBExecutionRole	2174
Using this policy	2174
Policy details	2175
Policy version	2175
JSON policy document	2175
Learn more	2175

AWSLambdaENIManagementAccess	2176
Using this policy	2176
Policy details	2176
Policy version	2176
JSON policy document	2176
Learn more	2177
AWSLambdaExecute	2177
Using this policy	2177
Policy details	2177
Policy version	2177
JSON policy document	2178
Learn more	2178
AWSLambdaFullAccess	2178
Using this policy	2179
Policy details	2179
Policy version	2179
JSON policy document	2179
Learn more	2181
AWSLambdaInvocation-DynamoDB	2181
Using this policy	2181
Policy details	2181
Policy version	2181
JSON policy document	2182
Learn more	2182
AWSLambdaKinesisExecutionRole	2182
Using this policy	2183
Policy details	2183
Policy version	2183
JSON policy document	2183
Learn more	2184
AWSLambdaMSKExecutionRole	2184
Using this policy	2184
Policy details	2184
Policy version	2184
JSON policy document	2185
Learn more	2185

AWSLambdaReplicator	2185
Using this policy	2186
Policy details	2186
Policy version	2186
JSON policy document	2186
Learn more	2187
AWSLambdaRole	2187
Using this policy	2187
Policy details	2188
Policy version	2188
JSON policy document	2188
Learn more	2188
AWSLambdaSQSQueueExecutionRole	2189
Using this policy	2189
Policy details	2189
Policy version	2189
JSON policy document	2189
Learn more	2190
AWSLambdaVPCLambdaAccessExecutionRole	2190
Using this policy	2190
Policy details	2190
Policy version	2190
JSON policy document	2191
Learn more	2191
AWSLicenseManagerConsumptionPolicy	2191
Using this policy	2192
Policy details	2192
Policy version	2192
JSON policy document	2192
Learn more	2193
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	2193
Using this policy	2193
Policy details	2193
Policy version	2193
JSON policy document	2194
Learn more	2194

AWSLicenseManagerMasterAccountRolePolicy	2195
Using this policy	2195
Policy details	2195
Policy version	2195
JSON policy document	2195
Learn more	2200
AWSLicenseManagerMemberAccountRolePolicy	2200
Using this policy	2200
Policy details	2200
Policy version	2201
JSON policy document	2201
Learn more	2202
AWSLicenseManagerServiceRolePolicy	2202
Using this policy	2202
Policy details	2202
Policy version	2203
JSON policy document	2203
Learn more	2206
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	2206
Using this policy	2206
Policy details	2206
Policy version	2207
JSON policy document	2207
Learn more	2209
AWSM2ServicePolicy	2209
Using this policy	2209
Policy details	2209
Policy version	2209
JSON policy document	2210
Learn more	2211
AWSManagedServices_ContactsServiceRolePolicy	2211
Using this policy	2211
Policy details	2211
Policy version	2212
JSON policy document	2212
Learn more	2213

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	2213
Using this policy	2213
Policy details	2213
Policy version	2213
JSON policy document	2213
Learn more	2215
AWSManagedServices_EventsServiceRolePolicy	2215
Using this policy	2215
Policy details	2215
Policy version	2216
JSON policy document	2216
Learn more	2216
AWSManagedServicesDeploymentToolkitPolicy	2217
Using this policy	2217
Policy details	2217
Policy version	2217
JSON policy document	2217
Learn more	2219
AWSMarketplaceAmilngestion	2220
Using this policy	2220
Policy details	2220
Policy version	2220
JSON policy document	2220
Learn more	2221
AWSMarketplaceDeploymentServiceRolePolicy	2221
Using this policy	2221
Policy details	2221
Policy version	2222
JSON policy document	2222
Learn more	2223
AWSMarketplaceFullAccess	2223
Using this policy	2223
Policy details	2224
Policy version	2224
JSON policy document	2224
Learn more	2227

AWSMarketplaceGetEntitlements	2227
Using this policy	2227
Policy details	2228
Policy version	2228
JSON policy document	2228
Learn more	2228
AWSMarketplaceImageBuildFullAccess	2229
Using this policy	2229
Policy details	2229
Policy version	2229
JSON policy document	2229
Learn more	2233
AWSMarketplaceLicenseManagementServiceRolePolicy	2233
Using this policy	2233
Policy details	2233
Policy version	2233
JSON policy document	2234
Learn more	2234
AWSMarketplaceManageSubscriptions	2234
Using this policy	2235
Policy details	2235
Policy version	2235
JSON policy document	2235
Learn more	2236
AWSMarketplaceMeteringFullAccess	2236
Using this policy	2236
Policy details	2236
Policy version	2237
JSON policy document	2237
Learn more	2237
AWSMarketplaceMeteringRegisterUsage	2237
Using this policy	2238
Policy details	2238
Policy version	2238
JSON policy document	2238
Learn more	2238

AWSMarketplaceProcurementSystemAdminFullAccess	2239
Using this policy	2239
Policy details	2239
Policy version	2239
JSON policy document	2239
Learn more	2240
AWSMarketplacePurchaseOrdersServiceRolePolicy	2240
Using this policy	2240
Policy details	2240
Policy version	2241
JSON policy document	2241
Learn more	2241
AWSMarketplaceRead-only	2241
Using this policy	2242
Policy details	2242
Policy version	2242
JSON policy document	2242
Learn more	2243
AWSMarketplaceResaleAuthorizationServiceRolePolicy	2243
Using this policy	2244
Policy details	2244
Policy version	2244
JSON policy document	2244
Learn more	2246
AWSMarketplaceSellerFullAccess	2247
Using this policy	2247
Policy details	2247
Policy version	2247
JSON policy document	2247
Learn more	2251
AWSMarketplaceSellerProductsFullAccess	2251
Using this policy	2251
Policy details	2251
Policy version	2251
JSON policy document	2252
Learn more	2253

AWSMarketplaceSellerProductsReadOnly	2254
Using this policy	2254
Policy details	2254
Policy version	2254
JSON policy document	2254
Learn more	2255
AWSMediaConnectServicePolicy	2255
Using this policy	2255
Policy details	2255
Policy version	2256
JSON policy document	2256
Learn more	2257
AWSMediaTailorServiceRolePolicy	2257
Using this policy	2257
Policy details	2257
Policy version	2258
JSON policy document	2258
Learn more	2258
AWSMigrationHubDiscoveryAccess	2259
Using this policy	2259
Policy details	2259
Policy version	2259
JSON policy document	2259
Learn more	2260
AWSMigrationHubDMSAccess	2261
Using this policy	2261
Policy details	2261
Policy version	2261
JSON policy document	2261
Learn more	2262
AWSMigrationHubFullAccess	2262
Using this policy	2263
Policy details	2263
Policy version	2263
JSON policy document	2263
Learn more	2264

AWSMigrationHubOrchestratorConsoleFullAccess	2265
Using this policy	2265
Policy details	2265
Policy version	2265
JSON policy document	2265
Learn more	2268
AWSMigrationHubOrchestratorInstanceRolePolicy	2269
Using this policy	2269
Policy details	2269
Policy version	2269
JSON policy document	2269
Learn more	2270
AWSMigrationHubOrchestratorPlugin	2270
Using this policy	2270
Policy details	2270
Policy version	2271
JSON policy document	2271
Learn more	2272
AWSMigrationHubOrchestratorServiceRolePolicy	2272
Using this policy	2272
Policy details	2273
Policy version	2273
JSON policy document	2273
Learn more	2276
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	2277
Using this policy	2277
Policy details	2277
Policy version	2277
JSON policy document	2277
Learn more	2283
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	2283
Using this policy	2283
Policy details	2284
Policy version	2284
JSON policy document	2284
Learn more	2285

AWSMigrationHubRefactorSpacesFullAccess	2286
Using this policy	2286
Policy details	2286
Policy version	2286
JSON policy document	2286
Learn more	2293
AWSMigrationHubRefactorSpacesServiceRolePolicy	2293
Using this policy	2293
Policy details	2293
Policy version	2293
JSON policy document	2294
Learn more	2297
AWSMigrationHubSMSAccess	2298
Using this policy	2298
Policy details	2298
Policy version	2298
JSON policy document	2298
Learn more	2299
AWSMigrationHubStrategyCollector	2299
Using this policy	2300
Policy details	2300
Policy version	2300
JSON policy document	2300
Learn more	2302
AWSMigrationHubStrategyConsoleFullAccess	2303
Using this policy	2303
Policy details	2303
Policy version	2303
JSON policy document	2303
Learn more	2305
AWSMigrationHubStrategyServiceRolePolicy	2305
Using this policy	2305
Policy details	2305
Policy version	2306
JSON policy document	2306
Learn more	2307

AWSMobileHub_FullAccess	2307
Using this policy	2307
Policy details	2307
Policy version	2307
JSON policy document	2308
Learn more	2309
AWSMobileHub_ReadOnly	2309
Using this policy	2310
Policy details	2310
Policy version	2310
JSON policy document	2310
Learn more	2311
AWSMSKReplicatorExecutionRole	2311
Using this policy	2312
Policy details	2312
Policy version	2312
JSON policy document	2312
Learn more	2313
AWSNetworkFirewallServiceRolePolicy	2314
Using this policy	2314
Policy details	2314
Policy version	2314
JSON policy document	2314
Learn more	2316
AWSNetworkManagerCloudWANServiceRolePolicy	2316
Using this policy	2316
Policy details	2316
Policy version	2317
JSON policy document	2317
Learn more	2317
AWSNetworkManagerFullAccess	2317
Using this policy	2317
Policy details	2318
Policy version	2318
JSON policy document	2318
Learn more	2319

AWSNetworkManagerReadOnlyAccess	2319
Using this policy	2319
Policy details	2319
Policy version	2319
JSON policy document	2319
Learn more	2320
AWSNetworkManagerServiceRolePolicy	2320
Using this policy	2320
Policy details	2320
Policy version	2321
JSON policy document	2321
Learn more	2322
AWSOpsWorks_FullAccess	2322
Using this policy	2322
Policy details	2322
Policy version	2322
JSON policy document	2323
Learn more	2324
AWSOpsWorksCloudWatchLogs	2324
Using this policy	2324
Policy details	2324
Policy version	2324
JSON policy document	2324
Learn more	2325
AWSOpsWorksCMInstanceProfileRole	2325
Using this policy	2325
Policy details	2325
Policy version	2326
JSON policy document	2326
Learn more	2327
AWSOpsWorksCMServiceRole	2327
Using this policy	2327
Policy details	2327
Policy version	2327
JSON policy document	2328
Learn more	2332

AWSOpsWorksInstanceRegistration	2332
Using this policy	2332
Policy details	2332
Policy version	2332
JSON policy document	2333
Learn more	2333
AWSOpsWorksRegisterCLI_EC2	2333
Using this policy	2333
Policy details	2334
Policy version	2334
JSON policy document	2334
Learn more	2335
AWSOpsWorksRegisterCLI_OnPremises	2335
Using this policy	2335
Policy details	2335
Policy version	2335
JSON policy document	2336
Learn more	2337
AWSOrganizationsFullAccess	2337
Using this policy	2337
Policy details	2338
Policy version	2338
JSON policy document	2338
Learn more	2339
AWSOrganizationsReadOnlyAccess	2339
Using this policy	2339
Policy details	2339
Policy version	2340
JSON policy document	2340
Learn more	2340
AWSOrganizationsServiceTrustPolicy	2341
Using this policy	2341
Policy details	2341
Policy version	2341
JSON policy document	2341
Learn more	2342

AWSOutpostsAuthorizeServerPolicy	2342
Using this policy	2342
Policy details	2342
Policy version	2343
JSON policy document	2343
Learn more	2343
AWSOutpostsServiceRolePolicy	2343
Using this policy	2344
Policy details	2344
Policy version	2344
JSON policy document	2344
Learn more	2345
AWSPanoramaApplianceRolePolicy	2345
Using this policy	2345
Policy details	2345
Policy version	2345
JSON policy document	2345
Learn more	2346
AWSPanoramaApplianceServiceRolePolicy	2346
Using this policy	2346
Policy details	2346
Policy version	2347
JSON policy document	2347
Learn more	2348
AWSPanoramaFullAccess	2348
Using this policy	2349
Policy details	2349
Policy version	2349
JSON policy document	2349
Learn more	2352
AWSPanoramaGreengrassGroupRolePolicy	2352
Using this policy	2352
Policy details	2352
Policy version	2352
JSON policy document	2353
Learn more	2354

AWSPanoramaSageMakerRolePolicy	2354
Using this policy	2354
Policy details	2354
Policy version	2355
JSON policy document	2355
Learn more	2355
AWSPanoramaServiceLinkedRolePolicy	2355
Using this policy	2356
Policy details	2356
Policy version	2356
JSON policy document	2356
Learn more	2359
AWSPanoramaServiceRolePolicy	2359
Using this policy	2359
Policy details	2359
Policy version	2359
JSON policy document	2360
Learn more	2366
AWSPriceListServiceFullAccess	2367
Using this policy	2367
Policy details	2367
Policy version	2367
JSON policy document	2367
Learn more	2368
AWSPrivateCAAuditor	2368
Using this policy	2368
Policy details	2368
Policy version	2368
JSON policy document	2369
Learn more	2369
AWSPrivateCAFullAccess	2369
Using this policy	2370
Policy details	2370
Policy version	2370
JSON policy document	2370
Learn more	2370

AWSPriateCAPrivilegedUser	2371
Using this policy	2371
Policy details	2371
Policy version	2371
JSON policy document	2371
Learn more	2373
AWSPriateCARedOnly	2373
Using this policy	2373
Policy details	2373
Policy version	2373
JSON policy document	2373
Learn more	2374
AWSPriateCAUser	2374
Using this policy	2374
Policy details	2374
Policy version	2375
JSON policy document	2375
Learn more	2376
AWSPriateMarketplaceAdminFullAccess	2376
Using this policy	2376
Policy details	2376
Policy version	2377
JSON policy document	2377
Learn more	2378
AWSPriateMarketplaceRequests	2378
Using this policy	2379
Policy details	2379
Policy version	2379
JSON policy document	2379
Learn more	2379
AWSPriateNetworksServiceRolePolicy	2380
Using this policy	2380
Policy details	2380
Policy version	2380
JSON policy document	2380
Learn more	2381

AWSProtonCodeBuildProvisioningBasicAccess	2381
Using this policy	2381
Policy details	2381
Policy version	2381
JSON policy document	2382
Learn more	2382
AWSProtonCodeBuildProvisioningServiceRolePolicy	2382
Using this policy	2383
Policy details	2383
Policy version	2383
JSON policy document	2383
Learn more	2384
AWSProtonDeveloperAccess	2385
Using this policy	2385
Policy details	2385
Policy version	2385
JSON policy document	2385
Learn more	2388
AWSProtonFullAccess	2388
Using this policy	2388
Policy details	2388
Policy version	2388
JSON policy document	2388
Learn more	2391
AWSProtonReadOnlyAccess	2391
Using this policy	2391
Policy details	2391
Policy version	2391
JSON policy document	2391
Learn more	2393
AWSProtonServiceGitSyncServiceRolePolicy	2393
Using this policy	2393
Policy details	2393
Policy version	2394
JSON policy document	2394
Learn more	2394

AWSProtonSyncServiceRolePolicy	2395
Using this policy	2395
Policy details	2395
Policy version	2395
JSON policy document	2395
Learn more	2396
AWSPurchaseOrdersServiceRolePolicy	2397
Using this policy	2397
Policy details	2397
Policy version	2397
JSON policy document	2397
Learn more	2398
AWSQuickSetupCFGCPacksPermissionsBoundary	2398
Using this policy	2398
Policy details	2399
Policy version	2399
JSON policy document	2399
Learn more	2402
AWSQuickSetupDeploymentRolePolicy	2402
Using this policy	2402
Policy details	2402
Policy version	2402
JSON policy document	2403
Learn more	2410
AWSQuickSetupDevOpsGuruPermissionsBoundary	2411
Using this policy	2411
Policy details	2411
Policy version	2411
JSON policy document	2411
Learn more	2414
AWSQuickSetupDistributorPermissionsBoundary	2414
Using this policy	2414
Policy details	2415
Policy version	2415
JSON policy document	2415
Learn more	2421

AWSQuickSetupPatchPolicyBaselineAccess	2421
Using this policy	2421
Policy details	2421
Policy version	2421
JSON policy document	2422
Learn more	2422
AWSQuickSetupPatchPolicyDeploymentRolePolicy	2423
Using this policy	2423
Policy details	2423
Policy version	2423
JSON policy document	2423
Learn more	2431
AWSQuickSetupPatchPolicyPermissionsBoundary	2431
Using this policy	2432
Policy details	2432
Policy version	2432
JSON policy document	2432
Learn more	2440
AWSQuickSetupSchedulerPermissionsBoundary	2440
Using this policy	2441
Policy details	2441
Policy version	2441
JSON policy document	2441
Learn more	2444
AWSQuickSetupSSMHostMgmtPermissionsBoundary	2445
Using this policy	2445
Policy details	2445
Policy version	2445
JSON policy document	2445
Learn more	2451
AWSQuickSightAssetBundleExportPolicy	2451
Using this policy	2451
Policy details	2452
Policy version	2452
JSON policy document	2452
Learn more	2454

AWSQuickSightAssetBundleImportPolicy	2454
Using this policy	2454
Policy details	2455
Policy version	2455
JSON policy document	2455
Learn more	2458
AWSQuickSightAthenaAccess	2458
Using this policy	2458
Policy details	2458
Policy version	2458
JSON policy document	2459
Learn more	2461
AWSQuickSightDescribeRDS	2461
Using this policy	2461
Policy details	2461
Policy version	2462
JSON policy document	2462
Learn more	2462
AWSQuickSightDescribeRedshift	2462
Using this policy	2462
Policy details	2463
Policy version	2463
JSON policy document	2463
Learn more	2463
AWSQuickSightElasticsearchPolicy	2464
Using this policy	2464
Policy details	2464
Policy version	2464
JSON policy document	2464
Learn more	2465
AWSQuickSightIoTAnalyticsAccess	2465
Using this policy	2466
Policy details	2466
Policy version	2466
JSON policy document	2466
Learn more	2467

AWSQuickSightListIAM	2467
Using this policy	2467
Policy details	2467
Policy version	2467
JSON policy document	2467
Learn more	2468
AWSQuickSightOpenSearchPolicy	2468
Using this policy	2468
Policy details	2468
Policy version	2468
JSON policy document	2469
Learn more	2470
AWSQuickSightSageMakerPolicy	2470
Using this policy	2470
Policy details	2470
Policy version	2470
JSON policy document	2471
Learn more	2472
AWSQuickSightTimestreamPolicy	2472
Using this policy	2472
Policy details	2472
Policy version	2472
JSON policy document	2473
Learn more	2473
AWSReachabilityAnalyzerServiceRolePolicy	2473
Using this policy	2474
Policy details	2474
Policy version	2474
JSON policy document	2474
Learn more	2476
AWSRefactoringToolkitFullAccess	2477
Using this policy	2477
Policy details	2477
Policy version	2477
JSON policy document	2477
Learn more	2491

AWSRefactoringToolkitSidecarPolicy	2491
Using this policy	2491
Policy details	2491
Policy version	2492
JSON policy document	2492
Learn more	2493
AWSrePostPrivateCloudWatchAccess	2493
Using this policy	2493
Policy details	2493
Policy version	2493
JSON policy document	2494
Learn more	2494
AWSRepostSpaceSupportOperationsPolicy	2494
Using this policy	2495
Policy details	2495
Policy version	2495
JSON policy document	2495
Learn more	2496
AWSResilienceHubAssessmentExecutionPolicy	2496
Using this policy	2496
Policy details	2496
Policy version	2496
JSON policy document	2496
Learn more	2501
AWSResourceAccessManagerFullAccess	2501
Using this policy	2501
Policy details	2501
Policy version	2501
JSON policy document	2501
Learn more	2502
AWSResourceAccessManagerReadOnlyAccess	2502
Using this policy	2502
Policy details	2502
Policy version	2502
JSON policy document	2503
Learn more	2503

AWSResourceAccessManagerResourceShareParticipantAccess	2503
Using this policy	2503
Policy details	2504
Policy version	2504
JSON policy document	2504
Learn more	2505
AWSResourceAccessManagerServiceRolePolicy	2505
Using this policy	2505
Policy details	2505
Policy version	2505
JSON policy document	2506
Learn more	2506
AWSResourceExplorerFullAccess	2507
Using this policy	2507
Policy details	2507
Policy version	2507
JSON policy document	2507
Learn more	2508
AWSResourceExplorerOrganizationsAccess	2508
Using this policy	2508
Policy details	2509
Policy version	2509
JSON policy document	2509
Learn more	2511
AWSResourceExplorerReadOnlyAccess	2511
Using this policy	2511
Policy details	2511
Policy version	2511
JSON policy document	2511
Learn more	2512
AWSResourceExplorerServiceRolePolicy	2512
Using this policy	2512
Policy details	2513
Policy version	2513
JSON policy document	2513
Learn more	2522

AWSResourceGroupsReadOnlyAccess	2522
Using this policy	2522
Policy details	2522
Policy version	2523
JSON policy document	2523
Learn more	2524
AWSRoboMaker_FullAccess	2524
Using this policy	2525
Policy details	2525
Policy version	2525
JSON policy document	2525
Learn more	2526
AWSRoboMakerReadOnlyAccess	2527
Using this policy	2527
Policy details	2527
Policy version	2527
JSON policy document	2527
Learn more	2528
AWSRoboMakerServicePolicy	2528
Using this policy	2528
Policy details	2528
Policy version	2528
JSON policy document	2529
Learn more	2530
AWSRoboMakerServiceRolePolicy	2530
Using this policy	2530
Policy details	2531
Policy version	2531
JSON policy document	2531
Learn more	2532
AWSRolesAnywhereServicePolicy	2532
Using this policy	2533
Policy details	2533
Policy version	2533
JSON policy document	2533
Learn more	2534

AWSS3OnOutpostsServiceRolePolicy	2534
Using this policy	2534
Policy details	2534
Policy version	2535
JSON policy document	2535
Learn more	2537
AWSSavingsPlansFullAccess	2537
Using this policy	2538
Policy details	2538
Policy version	2538
JSON policy document	2538
Learn more	2538
AWSSavingsPlansReadOnlyAccess	2539
Using this policy	2539
Policy details	2539
Policy version	2539
JSON policy document	2539
Learn more	2540
AWSSecurityHubFullAccess	2540
Using this policy	2540
Policy details	2540
Policy version	2540
JSON policy document	2541
Learn more	2541
AWSSecurityHubOrganizationsAccess	2542
Using this policy	2542
Policy details	2542
Policy version	2542
JSON policy document	2542
Learn more	2543
AWSSecurityHubReadOnlyAccess	2544
Using this policy	2544
Policy details	2544
Policy version	2544
JSON policy document	2544
Learn more	2545

AWSSecurityHubServiceRolePolicy	2545
Using this policy	2545
Policy details	2545
Policy version	2545
JSON policy document	2546
Learn more	2548
AWSServiceCatalogAdminFullAccess	2548
Using this policy	2548
Policy details	2548
Policy version	2548
JSON policy document	2548
Learn more	2551
AWSServiceCatalogAdminReadOnlyAccess	2551
Using this policy	2551
Policy details	2552
Policy version	2552
JSON policy document	2552
Learn more	2553
AWSServiceCatalogAppRegistryFullAccess	2553
Using this policy	2554
Policy details	2554
Policy version	2554
JSON policy document	2554
Learn more	2556
AWSServiceCatalogAppRegistryReadOnlyAccess	2556
Using this policy	2557
Policy details	2557
Policy version	2557
JSON policy document	2557
Learn more	2558
AWSServiceCatalogAppRegistryServiceRolePolicy	2558
Using this policy	2558
Policy details	2558
Policy version	2558
JSON policy document	2559
Learn more	2560

AWSServiceCatalogEndUserFullAccess	2560
Using this policy	2560
Policy details	2560
Policy version	2560
JSON policy document	2561
Learn more	2563
AWSServiceCatalogEndUserReadOnlyAccess	2563
Using this policy	2563
Policy details	2563
Policy version	2563
JSON policy document	2563
Learn more	2565
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	2565
Using this policy	2565
Policy details	2566
Policy version	2566
JSON policy document	2566
Learn more	2567
AWSServiceCatalogSyncServiceRolePolicy	2567
Using this policy	2567
Policy details	2567
Policy version	2567
JSON policy document	2567
Learn more	2568
AWSServiceRoleForAmazonEKSNodegroup	2569
Using this policy	2569
Policy details	2569
Policy version	2569
JSON policy document	2569
Learn more	2573
AWSServiceRoleForAmazonQDeveloper	2574
Using this policy	2574
Policy details	2574
Policy version	2574
JSON policy document	2574
Learn more	2575

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy	2575
Using this policy	2575
Policy details	2575
Policy version	2576
JSON policy document	2576
Learn more	2576
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy	2576
Using this policy	2576
Policy details	2577
Policy version	2577
JSON policy document	2577
Learn more	2577
AWSServiceRoleForCodeGuru-Profiler	2578
Using this policy	2578
Policy details	2578
Policy version	2578
JSON policy document	2578
Learn more	2579
AWSServiceRoleForCodeWhispererPolicy	2579
Using this policy	2579
Policy details	2579
Policy version	2579
JSON policy document	2580
Learn more	2581
AWSServiceRoleForEC2ScheduledInstances	2582
Using this policy	2582
Policy details	2582
Policy version	2582
JSON policy document	2582
Learn more	2583
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	2583
Using this policy	2583
Policy details	2584
Policy version	2584
JSON policy document	2584
Learn more	2584

AWSServiceRoleForImageBuilder	2585
Using this policy	2585
Policy details	2585
Policy version	2585
JSON policy document	2585
Learn more	2595
AWSServiceRoleForIoTSiteWise	2595
Using this policy	2595
Policy details	2595
Policy version	2595
JSON policy document	2596
Learn more	2597
AWSServiceRoleForLogDeliveryPolicy	2597
Using this policy	2597
Policy details	2597
Policy version	2598
JSON policy document	2598
Learn more	2598
AWSServiceRoleForMonitronPolicy	2598
Using this policy	2599
Policy details	2599
Policy version	2599
JSON policy document	2599
Learn more	2600
AWSServiceRoleForNeptuneGraphPolicy	2600
Using this policy	2600
Policy details	2600
Policy version	2600
JSON policy document	2601
Learn more	2602
AWSServiceRoleForPrivateMarketplaceAdminPolicy	2602
Using this policy	2602
Policy details	2602
Policy version	2603
JSON policy document	2603
Learn more	2604

AWSServiceRoleForSMS	2605
Using this policy	2605
Policy details	2605
Policy version	2605
JSON policy document	2605
Learn more	2612
AWSServiceRoleForUserSubscriptions	2612
Using this policy	2612
Policy details	2612
Policy version	2613
JSON policy document	2613
Learn more	2613
AWSServiceRolePolicyForBackupReports	2614
Using this policy	2614
Policy details	2614
Policy version	2614
JSON policy document	2614
Learn more	2615
AWSServiceRolePolicyForBackupRestoreTesting	2616
Using this policy	2616
Policy details	2616
Policy version	2616
JSON policy document	2616
Learn more	2619
AWSShieldDRTAcessPolicy	2619
Using this policy	2619
Policy details	2619
Policy version	2620
JSON policy document	2620
Learn more	2621
AWSShieldServiceRolePolicy	2621
Using this policy	2621
Policy details	2621
Policy version	2621
JSON policy document	2622
Learn more	2622

AWSSSMForSAPServiceLinkedRolePolicy	2622
Using this policy	2623
Policy details	2623
Policy version	2623
JSON policy document	2623
Learn more	2630
AWSSSMOpsInsightsServiceRolePolicy	2630
Using this policy	2630
Policy details	2630
Policy version	2630
JSON policy document	2630
Learn more	2631
AWSSSODirectoryAdministrator	2631
Using this policy	2631
Policy details	2632
Policy version	2632
JSON policy document	2632
Learn more	2632
AWSSSODirectoryReadOnly	2633
Using this policy	2633
Policy details	2633
Policy version	2633
JSON policy document	2633
Learn more	2634
AWSSSOMasterAccountAdministrator	2634
Using this policy	2634
Policy details	2634
Policy version	2635
JSON policy document	2635
Learn more	2637
AWSSSOMemberAccountAdministrator	2637
Using this policy	2637
Policy details	2637
Policy version	2637
JSON policy document	2637
Learn more	2639

AWSSSOReadOnly	2639
Using this policy	2639
Policy details	2639
Policy version	2639
JSON policy document	2640
Learn more	2640
AWSSSOServiceRolePolicy	2641
Using this policy	2641
Policy details	2641
Policy version	2641
JSON policy document	2641
Learn more	2645
AWSStepFunctionsConsoleFullAccess	2645
Using this policy	2645
Policy details	2645
Policy version	2645
JSON policy document	2646
Learn more	2646
AWSStepFunctionsFullAccess	2647
Using this policy	2647
Policy details	2647
Policy version	2647
JSON policy document	2647
Learn more	2648
AWSStepFunctionsReadOnlyAccess	2648
Using this policy	2648
Policy details	2648
Policy version	2648
JSON policy document	2649
Learn more	2649
AWSStorageGatewayFullAccess	2649
Using this policy	2650
Policy details	2650
Policy version	2650
JSON policy document	2650
Learn more	2651

AWSStrorageGatewayReadOnlyAccess	2651
Using this policy	2651
Policy details	2651
Policy version	2651
JSON policy document	2652
Learn more	2652
AWSStrorageGatewayServiceRolePolicy	2653
Using this policy	2653
Policy details	2653
Policy version	2653
JSON policy document	2653
Learn more	2654
AWSSupplyChainFederationAdminAccess	2654
Using this policy	2654
Policy details	2654
Policy version	2654
JSON policy document	2655
Learn more	2660
AWSSupportAccess	2660
Using this policy	2660
Policy details	2660
Policy version	2661
JSON policy document	2661
Learn more	2661
AWSSupportAppFullAccess	2661
Using this policy	2662
Policy details	2662
Policy version	2662
JSON policy document	2662
Learn more	2663
AWSSupportAppReadOnlyAccess	2663
Using this policy	2663
Policy details	2663
Policy version	2664
JSON policy document	2664
Learn more	2664

AWSSupportPlansFullAccess	2664
Using this policy	2664
Policy details	2665
Policy version	2665
JSON policy document	2665
Learn more	2665
AWSSupportPlansReadOnlyAccess	2666
Using this policy	2666
Policy details	2666
Policy version	2666
JSON policy document	2666
Learn more	2667
AWSSupportServiceRolePolicy	2667
Using this policy	2667
Policy details	2667
Policy version	2667
JSON policy document	2668
Learn more	2743
AWSSystemsManagerAccountDiscoveryServicePolicy	2743
Using this policy	2743
Policy details	2743
Policy version	2744
JSON policy document	2744
Learn more	2744
AWSSystemsManagerChangeManagementServicePolicy	2745
Using this policy	2745
Policy details	2745
Policy version	2745
JSON policy document	2745
Learn more	2747
AWSSystemsManagerEnableConfigRecordingExecutionPolicy	2747
Using this policy	2747
Policy details	2747
Policy version	2748
JSON policy document	2748
Learn more	2750

AWSSystemsManagerEnableExplorerExecutionPolicy	2750
Using this policy	2750
Policy details	2750
Policy version	2751
JSON policy document	2751
Learn more	2752
AWSSystemsManagerForSAPFullAccess	2752
Using this policy	2752
Policy details	2752
Policy version	2753
JSON policy document	2753
Learn more	2754
AWSSystemsManagerForSAPReadOnlyAccess	2754
Using this policy	2754
Policy details	2754
Policy version	2754
JSON policy document	2754
Learn more	2755
AWSSystemsManagerOpsDataSyncServiceRolePolicy	2755
Using this policy	2755
Policy details	2755
Policy version	2756
JSON policy document	2756
Learn more	2759
AWSThinkboxAssetServerPolicy	2760
Using this policy	2760
Policy details	2760
Policy version	2760
JSON policy document	2760
Learn more	2761
AWSThinkboxAWSPortalAdminPolicy	2761
Using this policy	2761
Policy details	2761
Policy version	2762
JSON policy document	2762
Learn more	2772

AWSThinkboxAWSPortalGatewayPolicy	2772
Using this policy	2772
Policy details	2772
Policy version	2772
JSON policy document	2773
Learn more	2774
AWSThinkboxAWSPortalWorkerPolicy	2775
Using this policy	2775
Policy details	2775
Policy version	2775
JSON policy document	2775
Learn more	2777
AWSThinkboxDeadlineResourceTrackerAccessPolicy	2777
Using this policy	2778
Policy details	2778
Policy version	2778
JSON policy document	2778
Learn more	2781
AWSThinkboxDeadlineResourceTrackerAdminPolicy	2781
Using this policy	2781
Policy details	2781
Policy version	2781
JSON policy document	2782
Learn more	2787
AWSThinkboxDeadlineSpotEventPluginAdminPolicy	2788
Using this policy	2788
Policy details	2788
Policy version	2788
JSON policy document	2788
Learn more	2791
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	2791
Using this policy	2792
Policy details	2792
Policy version	2792
JSON policy document	2792
Learn more	2793

AWSTransferConsoleFullAccess	2794
Using this policy	2794
Policy details	2794
Policy version	2794
JSON policy document	2794
Learn more	2795
AWSTransferFullAccess	2795
Using this policy	2796
Policy details	2796
Policy version	2796
JSON policy document	2796
Learn more	2797
AWSTransferLoggingAccess	2797
Using this policy	2797
Policy details	2797
Policy version	2798
JSON policy document	2798
Learn more	2798
AWSTransferReadOnlyAccess	2798
Using this policy	2799
Policy details	2799
Policy version	2799
JSON policy document	2799
Learn more	2800
AWSTrustedAdvisorPriorityFullAccess	2800
Using this policy	2800
Policy details	2800
Policy version	2800
JSON policy document	2800
Learn more	2802
AWSTrustedAdvisorPriorityReadOnlyAccess	2802
Using this policy	2803
Policy details	2803
Policy version	2803
JSON policy document	2803
Learn more	2804

AWSTrustedAdvisorReportingServiceRolePolicy	2804
Using this policy	2804
Policy details	2805
Policy version	2805
JSON policy document	2805
Learn more	2806
AWSTrustedAdvisorServiceRolePolicy	2806
Using this policy	2806
Policy details	2806
Policy version	2806
JSON policy document	2806
Learn more	2809
AWSUserNotificationsServiceLinkedRolePolicy	2809
Using this policy	2810
Policy details	2810
Policy version	2810
JSON policy document	2810
Learn more	2811
AWSVendorInsightsAssessorFullAccess	2811
Using this policy	2811
Policy details	2811
Policy version	2811
JSON policy document	2812
Learn more	2813
AWSVendorInsightsAssessorReadOnly	2813
Using this policy	2813
Policy details	2813
Policy version	2813
JSON policy document	2814
Learn more	2814
AWSVendorInsightsVendorFullAccess	2814
Using this policy	2815
Policy details	2815
Policy version	2815
JSON policy document	2815
Learn more	2817

AWSVendorInsightsVendorReadOnly	2817
Using this policy	2817
Policy details	2817
Policy version	2817
JSON policy document	2818
Learn more	2819
AWSVpcLatticeServiceRolePolicy	2819
Using this policy	2819
Policy details	2819
Policy version	2819
JSON policy document	2819
Learn more	2820
AWSVPCS2SVpnServiceRolePolicy	2820
Using this policy	2820
Policy details	2820
Policy version	2821
JSON policy document	2821
Learn more	2821
AWSVPCTransitGatewayServiceRolePolicy	2821
Using this policy	2822
Policy details	2822
Policy version	2822
JSON policy document	2822
Learn more	2823
AWSVPCVerifiedAccessServiceRolePolicy	2823
Using this policy	2823
Policy details	2823
Policy version	2823
JSON policy document	2824
Learn more	2825
AWSWAFConsoleFullAccess	2825
Using this policy	2826
Policy details	2826
Policy version	2826
JSON policy document	2826
Learn more	2828

AWSWAFConsoleReadOnlyAccess	2828
Using this policy	2828
Policy details	2829
Policy version	2829
JSON policy document	2829
Learn more	2830
AWSWAFFullAccess	2830
Using this policy	2830
Policy details	2830
Policy version	2831
JSON policy document	2831
Learn more	2832
AWSWAFReadOnlyAccess	2833
Using this policy	2833
Policy details	2833
Policy version	2833
JSON policy document	2833
Learn more	2834
AWSWellArchitectedDiscoveryServiceRolePolicy	2834
Using this policy	2834
Policy details	2834
Policy version	2835
JSON policy document	2835
Learn more	2836
AWSWellArchitectedOrganizationsServiceRolePolicy	2836
Using this policy	2837
Policy details	2837
Policy version	2837
JSON policy document	2837
Learn more	2838
AWSWickrFullAccess	2838
Using this policy	2838
Policy details	2838
Policy version	2838
JSON policy document	2838
Learn more	2839

AWSXrayCrossAccountSharingConfiguration	2839
Using this policy	2839
Policy details	2839
Policy version	2839
JSON policy document	2840
Learn more	2841
AWSXRayDaemonWriteAccess	2841
Using this policy	2841
Policy details	2841
Policy version	2841
JSON policy document	2841
Learn more	2842
AWSXrayFullAccess	2842
Using this policy	2842
Policy details	2842
Policy version	2843
JSON policy document	2843
Learn more	2843
AWSXrayReadOnlyAccess	2844
Using this policy	2844
Policy details	2844
Policy version	2844
JSON policy document	2844
Learn more	2845
AWSXrayWriteOnlyAccess	2845
Using this policy	2845
Policy details	2845
Policy version	2846
JSON policy document	2846
Learn more	2846
AWSZonalAutoshiftPracticeRunSLRPolicy	2847
Using this policy	2847
Policy details	2847
Policy version	2847
JSON policy document	2847
Learn more	2848

BatchServiceRolePolicy	2848
Using this policy	2848
Policy details	2848
Policy version	2849
JSON policy document	2849
Learn more	2855
Billing	2855
Using this policy	2855
Policy details	2855
Policy version	2855
JSON policy document	2856
Learn more	2858
CertificateManagerServiceRolePolicy	2859
Using this policy	2859
Policy details	2859
Policy version	2859
JSON policy document	2859
Learn more	2860
ClientVPNServiceConnectionsRolePolicy	2860
Using this policy	2860
Policy details	2860
Policy version	2860
JSON policy document	2861
Learn more	2861
ClientVPNServiceRolePolicy	2861
Using this policy	2861
Policy details	2861
Policy version	2862
JSON policy document	2862
Learn more	2863
CloudFormationStackSetsOrgAdminServiceRolePolicy	2863
Using this policy	2863
Policy details	2863
Policy version	2863
JSON policy document	2864
Learn more	2864

CloudFormationStackSetsOrgMemberServiceRolePolicy	2864
Using this policy	2864
Policy details	2865
Policy version	2865
JSON policy document	2865
Learn more	2866
CloudFrontFullAccess	2866
Using this policy	2866
Policy details	2866
Policy version	2866
JSON policy document	2867
Learn more	2868
CloudFrontReadOnlyAccess	2868
Using this policy	2868
Policy details	2868
Policy version	2868
JSON policy document	2869
Learn more	2869
CloudHSMServiceRolePolicy	2870
Using this policy	2870
Policy details	2870
Policy version	2870
JSON policy document	2870
Learn more	2871
CloudSearchFullAccess	2871
Using this policy	2871
Policy details	2871
Policy version	2871
JSON policy document	2872
Learn more	2872
CloudSearchReadOnlyAccess	2872
Using this policy	2872
Policy details	2872
Policy version	2873
JSON policy document	2873
Learn more	2873

CloudTrailServiceRolePolicy	2873
Using this policy	2874
Policy details	2874
Policy version	2874
JSON policy document	2874
Learn more	2876
CloudWatch-CrossAccountAccess	2876
Using this policy	2876
Policy details	2876
Policy version	2876
JSON policy document	2877
Learn more	2877
CloudWatchActionsEC2Access	2877
Using this policy	2877
Policy details	2877
Policy version	2878
JSON policy document	2878
Learn more	2878
CloudWatchAgentAdminPolicy	2878
Using this policy	2879
Policy details	2879
Policy version	2879
JSON policy document	2879
Learn more	2880
CloudWatchAgentServerPolicy	2880
Using this policy	2880
Policy details	2880
Policy version	2881
JSON policy document	2881
Learn more	2882
CloudWatchApplicationInsightsFullAccess	2882
Using this policy	2882
Policy details	2882
Policy version	2882
JSON policy document	2883
Learn more	2884

CloudWatchApplicationInsightsReadOnlyAccess	2884
Using this policy	2884
Policy details	2884
Policy version	2885
JSON policy document	2885
Learn more	2885
CloudwatchApplicationInsightsServiceLinkedRolePolicy	2885
Using this policy	2886
Policy details	2886
Policy version	2886
JSON policy document	2886
Learn more	2896
CloudWatchApplicationSignalsFullAccess	2896
Using this policy	2896
Policy details	2896
Policy version	2896
JSON policy document	2897
Learn more	2899
CloudWatchApplicationSignalsReadOnlyAccess	2900
Using this policy	2900
Policy details	2900
Policy version	2900
JSON policy document	2900
Learn more	2903
CloudWatchApplicationSignalsServiceRolePolicy	2903
Using this policy	2903
Policy details	2903
Policy version	2903
JSON policy document	2904
Learn more	2906
CloudWatchAutomaticDashboardsAccess	2906
Using this policy	2906
Policy details	2906
Policy version	2906
JSON policy document	2907
Learn more	2908

CloudWatchCrossAccountSharingConfiguration	2908
Using this policy	2908
Policy details	2908
Policy version	2909
JSON policy document	2909
Learn more	2910
CloudWatchEventsBuiltInTargetExecutionAccess	2910
Using this policy	2910
Policy details	2910
Policy version	2910
JSON policy document	2911
Learn more	2911
CloudWatchEventsFullAccess	2911
Using this policy	2911
Policy details	2911
Policy version	2912
JSON policy document	2912
Learn more	2914
CloudWatchEventsInvocationAccess	2914
Using this policy	2914
Policy details	2914
Policy version	2914
JSON policy document	2915
Learn more	2915
CloudWatchEventsReadOnlyAccess	2915
Using this policy	2915
Policy details	2916
Policy version	2916
JSON policy document	2916
Learn more	2917
CloudWatchEventsServiceRolePolicy	2918
Using this policy	2918
Policy details	2918
Policy version	2918
JSON policy document	2918
Learn more	2919

CloudWatchFullAccess	2919
Using this policy	2919
Policy details	2919
Policy version	2919
JSON policy document	2920
Learn more	2921
CloudWatchFullAccessV2	2921
Using this policy	2921
Policy details	2921
Policy version	2921
JSON policy document	2921
Learn more	2923
CloudWatchInternetMonitorServiceRolePolicy	2923
Using this policy	2923
Policy details	2924
Policy version	2924
JSON policy document	2924
Learn more	2925
CloudWatchLambdaInsightsExecutionRolePolicy	2925
Using this policy	2925
Policy details	2925
Policy version	2926
JSON policy document	2926
Learn more	2926
CloudWatchLogsCrossAccountSharingConfiguration	2927
Using this policy	2927
Policy details	2927
Policy version	2927
JSON policy document	2927
Learn more	2928
CloudWatchLogsFullAccess	2928
Using this policy	2928
Policy details	2929
Policy version	2929
JSON policy document	2929
Learn more	2929

CloudWatchLogsReadOnlyAccess	2930
Using this policy	2930
Policy details	2930
Policy version	2930
JSON policy document	2930
Learn more	2931
CloudWatchNetworkMonitorServiceRolePolicy	2931
Using this policy	2931
Policy details	2931
Policy version	2932
JSON policy document	2932
Learn more	2933
CloudWatchReadOnlyAccess	2933
Using this policy	2933
Policy details	2933
Policy version	2934
JSON policy document	2934
Learn more	2935
CloudWatchSyntheticsFullAccess	2935
Using this policy	2935
Policy details	2936
Policy version	2936
JSON policy document	2936
Learn more	2941
CloudWatchSyntheticsReadOnlyAccess	2941
Using this policy	2941
Policy details	2941
Policy version	2941
JSON policy document	2941
Learn more	2942
ComprehendDataAccessRolePolicy	2942
Using this policy	2942
Policy details	2942
Policy version	2943
JSON policy document	2943
Learn more	2943

ComprehendFullAccess	2943
Using this policy	2944
Policy details	2944
Policy version	2944
JSON policy document	2944
Learn more	2945
ComprehendMedicalFullAccess	2945
Using this policy	2945
Policy details	2945
Policy version	2945
JSON policy document	2945
Learn more	2946
ComprehendReadOnly	2946
Using this policy	2946
Policy details	2946
Policy version	2946
JSON policy document	2947
Learn more	2948
ComputeOptimizerReadOnlyAccess	2948
Using this policy	2948
Policy details	2948
Policy version	2949
JSON policy document	2949
Learn more	2950
ComputeOptimizerServiceRolePolicy	2950
Using this policy	2950
Policy details	2950
Policy version	2951
JSON policy document	2951
Learn more	2952
ConfigConformsServiceRolePolicy	2952
Using this policy	2952
Policy details	2952
Policy version	2953
JSON policy document	2953
Learn more	2956

CostOptimizationHubAdminAccess	2956
Using this policy	2956
Policy details	2956
Policy version	2956
JSON policy document	2956
Learn more	2958
CostOptimizationHubReadOnlyAccess	2958
Using this policy	2958
Policy details	2958
Policy version	2958
JSON policy document	2959
Learn more	2959
CostOptimizationHubServiceRolePolicy	2959
Using this policy	2959
Policy details	2960
Policy version	2960
JSON policy document	2960
Learn more	2961
CustomerProfilesServiceLinkedRolePolicy	2961
Using this policy	2961
Policy details	2961
Policy version	2961
JSON policy document	2962
Learn more	2962
DatabaseAdministrator	2963
Using this policy	2963
Policy details	2963
Policy version	2963
JSON policy document	2963
Learn more	2966
DataScientist	2966
Using this policy	2966
Policy details	2966
Policy version	2966
JSON policy document	2966
Learn more	2970

DAXServiceRolePolicy	2970
Using this policy	2970
Policy details	2971
Policy version	2971
JSON policy document	2971
Learn more	2972
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	2972
Using this policy	2972
Policy details	2972
Policy version	2972
JSON policy document	2972
Learn more	2973
DynamoDBKinesisReplicationServiceRolePolicy	2973
Using this policy	2973
Policy details	2973
Policy version	2974
JSON policy document	2974
Learn more	2974
DynamoDBReplicationServiceRolePolicy	2975
Using this policy	2975
Policy details	2975
Policy version	2975
JSON policy document	2975
Learn more	2976
EC2FastLaunchFullAccess	2977
Using this policy	2977
Policy details	2977
Policy version	2977
JSON policy document	2977
Learn more	2980
EC2FastLaunchServiceRolePolicy	2980
Using this policy	2980
Policy details	2980
Policy version	2981
JSON policy document	2981
Learn more	2985

EC2FleetTimeShiftableServiceRolePolicy	2985
Using this policy	2985
Policy details	2985
Policy version	2985
JSON policy document	2985
Learn more	2987
Ec2ImageBuilderCrossAccountDistributionAccess	2987
Using this policy	2987
Policy details	2987
Policy version	2987
JSON policy document	2988
Learn more	2988
EC2ImageBuilderLifecycleExecutionPolicy	2988
Using this policy	2989
Policy details	2989
Policy version	2989
JSON policy document	2989
Learn more	2991
EC2InstanceConnect	2991
Using this policy	2991
Policy details	2992
Policy version	2992
JSON policy document	2992
Learn more	2992
Ec2InstanceConnectEndpoint	2993
Using this policy	2993
Policy details	2993
Policy version	2993
JSON policy document	2993
Learn more	2995
EC2InstanceProfileForImageBuilder	2995
Using this policy	2996
Policy details	2996
Policy version	2996
JSON policy document	2996
Learn more	2997

EC2InstanceProfileForImageBuilderECRContainerBuilds	2997
Using this policy	2998
Policy details	2998
Policy version	2998
JSON policy document	2998
Learn more	2999
ECRReplicationServiceRolePolicy	3000
Using this policy	3000
Policy details	3000
Policy version	3000
JSON policy document	3000
Learn more	3001
ECRTemplateServiceRolePolicy	3001
Using this policy	3001
Policy details	3001
Policy version	3001
JSON policy document	3002
Learn more	3002
ElastiCacheServiceRolePolicy	3002
Using this policy	3002
Policy details	3002
Policy version	3003
JSON policy document	3003
Learn more	3005
ElasticLoadBalancingFullAccess	3005
Using this policy	3005
Policy details	3005
Policy version	3005
JSON policy document	3005
Learn more	3007
ElasticLoadBalancingReadOnly	3007
Using this policy	3007
Policy details	3007
Policy version	3007
JSON policy document	3008
Learn more	3009

ElementalActivationsDownloadSoftwareAccess	3009
Using this policy	3009
Policy details	3009
Policy version	3009
JSON policy document	3010
Learn more	3010
ElementalActivationsFullAccess	3010
Using this policy	3010
Policy details	3010
Policy version	3011
JSON policy document	3011
Learn more	3011
ElementalActivationsGenerateLicenses	3011
Using this policy	3012
Policy details	3012
Policy version	3012
JSON policy document	3012
Learn more	3013
ElementalActivationsReadOnlyAccess	3013
Using this policy	3013
Policy details	3013
Policy version	3013
JSON policy document	3013
Learn more	3014
ElementalAppliancesSoftwareFullAccess	3014
Using this policy	3014
Policy details	3014
Policy version	3015
JSON policy document	3015
Learn more	3015
ElementalAppliancesSoftwareReadOnlyAccess	3015
Using this policy	3016
Policy details	3016
Policy version	3016
JSON policy document	3016
Learn more	3016

ElementalSupportCenterFullAccess	3017
Using this policy	3017
Policy details	3017
Policy version	3017
JSON policy document	3017
Learn more	3018
EMRDescribeClusterPolicyForEMRWAL	3018
Using this policy	3018
Policy details	3018
Policy version	3019
JSON policy document	3019
Learn more	3019
FMSServiceRolePolicy	3019
Using this policy	3019
Policy details	3020
Policy version	3020
JSON policy document	3020
Learn more	3036
FSxDeleteServiceLinkedRoleAccess	3036
Using this policy	3036
Policy details	3036
Policy version	3037
JSON policy document	3037
Learn more	3037
GameLiftGameServerGroupPolicy	3037
Using this policy	3038
Policy details	3038
Policy version	3038
JSON policy document	3038
Learn more	3040
GlobalAcceleratorFullAccess	3040
Using this policy	3040
Policy details	3040
Policy version	3040
JSON policy document	3040
Learn more	3041

GlobalAcceleratorReadOnlyAccess	3042
Using this policy	3042
Policy details	3042
Policy version	3042
JSON policy document	3042
Learn more	3043
GreengrassOTAUpdateArtifactAccess	3043
Using this policy	3043
Policy details	3043
Policy version	3043
JSON policy document	3044
Learn more	3044
GroundTruthSyntheticConsoleFullAccess	3044
Using this policy	3044
Policy details	3045
Policy version	3045
JSON policy document	3045
Learn more	3045
GroundTruthSyntheticConsoleReadOnlyAccess	3046
Using this policy	3046
Policy details	3046
Policy version	3046
JSON policy document	3046
Learn more	3047
Health_OrganizationsServiceRolePolicy	3047
Using this policy	3047
Policy details	3047
Policy version	3047
JSON policy document	3048
Learn more	3048
IAMAccessAdvisorReadOnly	3048
Using this policy	3048
Policy details	3048
Policy version	3049
JSON policy document	3049
Learn more	3050

IAMAccessAnalyzerFullAccess	3050
Using this policy	3050
Policy details	3050
Policy version	3050
JSON policy document	3051
Learn more	3052
IAMAccessAnalyzerReadOnlyAccess	3052
Using this policy	3052
Policy details	3052
Policy version	3052
JSON policy document	3052
Learn more	3053
IAMFullAccess	3053
Using this policy	3053
Policy details	3053
Policy version	3054
JSON policy document	3054
Learn more	3054
IAMReadOnlyAccess	3055
Using this policy	3055
Policy details	3055
Policy version	3055
JSON policy document	3055
Learn more	3056
IAMSelfManageServiceSpecificCredentials	3056
Using this policy	3056
Policy details	3056
Policy version	3056
JSON policy document	3057
Learn more	3057
IAMUserChangePassword	3057
Using this policy	3057
Policy details	3058
Policy version	3058
JSON policy document	3058
Learn more	3059

IAMUserSSHKeys	3059
Using this policy	3059
Policy details	3059
Policy version	3059
JSON policy document	3059
Learn more	3060
IVSFullAccess	3060
Using this policy	3060
Policy details	3060
Policy version	3061
JSON policy document	3061
Learn more	3061
IVSReadOnlyAccess	3061
Using this policy	3062
Policy details	3062
Policy version	3062
JSON policy document	3062
Learn more	3063
IVSRecordToS3	3063
Using this policy	3063
Policy details	3064
Policy version	3064
JSON policy document	3064
Learn more	3064
KafkaConnectServiceRolePolicy	3065
Using this policy	3065
Policy details	3065
Policy version	3065
JSON policy document	3065
Learn more	3067
KafkaServiceRolePolicy	3067
Using this policy	3067
Policy details	3067
Policy version	3067
JSON policy document	3067
Learn more	3069

KeyspacesReplicationServiceRolePolicy	3069
Using this policy	3069
Policy details	3069
Policy version	3070
JSON policy document	3070
Learn more	3070
LakeFormationDataAccessServiceRolePolicy	3070
Using this policy	3071
Policy details	3071
Policy version	3071
JSON policy document	3071
Learn more	3072
LexBotPolicy	3072
Using this policy	3072
Policy details	3072
Policy version	3072
JSON policy document	3072
Learn more	3073
LexChannelPolicy	3073
Using this policy	3073
Policy details	3073
Policy version	3074
JSON policy document	3074
Learn more	3074
LightsailExportAccess	3074
Using this policy	3075
Policy details	3075
Policy version	3075
JSON policy document	3075
Learn more	3076
MediaConnectGatewayInstanceRolePolicy	3076
Using this policy	3076
Policy details	3076
Policy version	3077
JSON policy document	3077
Learn more	3077

MediaPackageServiceRolePolicy	3077
Using this policy	3078
Policy details	3078
Policy version	3078
JSON policy document	3078
Learn more	3079
MemoryDBServiceRolePolicy	3079
Using this policy	3079
Policy details	3079
Policy version	3079
JSON policy document	3080
Learn more	3081
MigrationHubDMSAccessServiceRolePolicy	3082
Using this policy	3082
Policy details	3082
Policy version	3082
JSON policy document	3082
Learn more	3083
MigrationHubServiceRolePolicy	3083
Using this policy	3084
Policy details	3084
Policy version	3084
JSON policy document	3084
Learn more	3085
MigrationHubSMSAccessServiceRolePolicy	3086
Using this policy	3086
Policy details	3086
Policy version	3086
JSON policy document	3086
Learn more	3087
MonitronServiceRolePolicy	3087
Using this policy	3088
Policy details	3088
Policy version	3088
JSON policy document	3088
Learn more	3089

NeptuneConsoleFullAccess	3089
Using this policy	3089
Policy details	3089
Policy version	3089
JSON policy document	3089
Learn more	3095
NeptuneFullAccess	3095
Using this policy	3095
Policy details	3095
Policy version	3096
JSON policy document	3096
Learn more	3100
NeptuneGraphReadOnlyAccess	3100
Using this policy	3100
Policy details	3100
Policy version	3100
JSON policy document	3101
Learn more	3102
NeptuneReadOnlyAccess	3102
Using this policy	3102
Policy details	3102
Policy version	3103
JSON policy document	3103
Learn more	3105
NetworkAdministrator	3105
Using this policy	3105
Policy details	3105
Policy version	3106
JSON policy document	3106
Learn more	3113
OAMFullAccess	3113
Using this policy	3113
Policy details	3113
Policy version	3113
JSON policy document	3114
Learn more	3114

OAMReadOnlyAccess	3114
Using this policy	3114
Policy details	3114
Policy version	3115
JSON policy document	3115
Learn more	3115
OpensearchIngestionSelfManagedVpcePolicy	3115
Using this policy	3116
Policy details	3116
Policy version	3116
JSON policy document	3116
Learn more	3117
PartnerCentralAccountManagementUserRoleAssociation	3117
Using this policy	3117
Policy details	3117
Policy version	3117
JSON policy document	3118
Learn more	3118
PowerUserAccess	3119
Using this policy	3119
Policy details	3119
Policy version	3119
JSON policy document	3119
Learn more	3120
QBusinessServiceRolePolicy	3120
Using this policy	3120
Policy details	3120
Policy version	3121
JSON policy document	3121
Learn more	3122
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	3122
Using this policy	3123
Policy details	3123
Policy version	3123
JSON policy document	3123
Learn more	3124

RDSCloudHsmAuthorizationRole	3124
Using this policy	3124
Policy details	3124
Policy version	3124
JSON policy document	3125
Learn more	3125
ReadOnlyAccess	3125
Using this policy	3126
Policy details	3126
Policy version	3126
JSON policy document	3126
Learn more	3176
ResourceGroupsandTagEditorFullAccess	3176
Using this policy	3176
Policy details	3176
Policy version	3176
JSON policy document	3176
Learn more	3177
ResourceGroupsandTagEditorReadOnlyAccess	3177
Using this policy	3177
Policy details	3178
Policy version	3178
JSON policy document	3178
Learn more	3179
ResourceGroupsServiceRolePolicy	3179
Using this policy	3179
Policy details	3179
Policy version	3179
JSON policy document	3180
Learn more	3180
ROSAAmazonEBSCSIDriverOperatorPolicy	3180
Using this policy	3180
Policy details	3180
Policy version	3181
JSON policy document	3181
Learn more	3184

ROSACloudNetworkConfigOperatorPolicy	3184
Using this policy	3184
Policy details	3184
Policy version	3185
JSON policy document	3185
Learn more	3186
ROSAControlPlaneOperatorPolicy	3186
Using this policy	3186
Policy details	3186
Policy version	3186
JSON policy document	3187
Learn more	3191
ROSAImageRegistryOperatorPolicy	3191
Using this policy	3191
Policy details	3191
Policy version	3192
JSON policy document	3192
Learn more	3193
ROSAIngressOperatorPolicy	3193
Using this policy	3194
Policy details	3194
Policy version	3194
JSON policy document	3194
Learn more	3195
ROSAInstallerPolicy	3195
Using this policy	3195
Policy details	3195
Policy version	3196
JSON policy document	3196
Learn more	3204
ROSAKMSPProviderPolicy	3204
Using this policy	3204
Policy details	3204
Policy version	3204
JSON policy document	3204
Learn more	3205

ROSAKubeControllerPolicy	3205
Using this policy	3205
Policy details	3206
Policy version	3206
JSON policy document	3206
Learn more	3210
ROSAManageSubscription	3211
Using this policy	3211
Policy details	3211
Policy version	3211
JSON policy document	3211
Learn more	3212
ROSANodePoolManagementPolicy	3212
Using this policy	3212
Policy details	3212
Policy version	3213
JSON policy document	3213
Learn more	3218
ROSASRESupportPolicy	3219
Using this policy	3219
Policy details	3219
Policy version	3219
JSON policy document	3219
Learn more	3224
ROSAWorkerInstancePolicy	3224
Using this policy	3225
Policy details	3225
Policy version	3225
JSON policy document	3225
Learn more	3225
Route53RecoveryReadinessServiceRolePolicy	3226
Using this policy	3226
Policy details	3226
Policy version	3226
JSON policy document	3226
Learn more	3230

Route53ResolverServiceRolePolicy	3230
Using this policy	3230
Policy details	3230
Policy version	3230
JSON policy document	3231
Learn more	3231
S3StorageLensServiceRolePolicy	3231
Using this policy	3232
Policy details	3232
Policy version	3232
JSON policy document	3232
Learn more	3233
SecretsManagerReadWrite	3233
Using this policy	3233
Policy details	3233
Policy version	3233
JSON policy document	3233
Learn more	3235
SecurityAudit	3235
Using this policy	3235
Policy details	3236
Policy version	3236
JSON policy document	3236
Learn more	3253
SecurityLakeServiceLinkedRole	3253
Using this policy	3254
Policy details	3254
Policy version	3254
JSON policy document	3254
Learn more	3257
ServerMigration_ServiceRole	3257
Using this policy	3257
Policy details	3257
Policy version	3258
JSON policy document	3258
Learn more	3262

ServerMigrationConnector	3263
Using this policy	3263
Policy details	3263
Policy version	3263
JSON policy document	3263
Learn more	3265
ServerMigrationServiceConsoleFullAccess	3265
Using this policy	3265
Policy details	3265
Policy version	3266
JSON policy document	3266
Learn more	3267
ServerMigrationServiceLaunchRole	3268
Using this policy	3268
Policy details	3268
Policy version	3268
JSON policy document	3268
Learn more	3271
ServerMigrationServiceRoleForInstanceValidation	3271
Using this policy	3271
Policy details	3271
Policy version	3272
JSON policy document	3272
Learn more	3272
ServiceQuotasFullAccess	3273
Using this policy	3273
Policy details	3273
Policy version	3273
JSON policy document	3273
Learn more	3275
ServiceQuotasReadOnlyAccess	3275
Using this policy	3275
Policy details	3275
Policy version	3276
JSON policy document	3276
Learn more	3277

ServiceQuotasServiceRolePolicy	3277
Using this policy	3277
Policy details	3277
Policy version	3277
JSON policy document	3278
Learn more	3278
SimpleWorkflowFullAccess	3278
Using this policy	3278
Policy details	3278
Policy version	3279
JSON policy document	3279
Learn more	3279
SplitCostAllocationDataServiceRolePolicy	3279
Using this policy	3280
Policy details	3280
Policy version	3280
JSON policy document	3280
Learn more	3281
SSMQuickSetupRolePolicy	3281
Using this policy	3281
Policy details	3281
Policy version	3281
JSON policy document	3282
Learn more	3284
SupportUser	3284
Using this policy	3284
Policy details	3284
Policy version	3284
JSON policy document	3285
Learn more	3289
SystemAdministrator	3290
Using this policy	3290
Policy details	3290
Policy version	3290
JSON policy document	3290
Learn more	3296

TranslateFullAccess	3296
Using this policy	3297
Policy details	3297
Policy version	3297
JSON policy document	3297
Learn more	3298
TranslateReadOnly	3298
Using this policy	3298
Policy details	3298
Policy version	3298
JSON policy document	3299
Learn more	3299
ViewOnlyAccess	3299
Using this policy	3300
Policy details	3300
Policy version	3300
JSON policy document	3300
Learn more	3309
VMImportExportRoleForAWSConnector	3309
Using this policy	3309
Policy details	3309
Policy version	3309
JSON policy document	3310
Learn more	3310
VPCLatticeFullAccess	3311
Using this policy	3311
Policy details	3311
Policy version	3311
JSON policy document	3311
Learn more	3313
VPCLatticeReadOnlyAccess	3313
Using this policy	3314
Policy details	3314
Policy version	3314
JSON policy document	3314
Learn more	3315

VPCLatticeServicesInvokeAccess	3315
Using this policy	3315
Policy details	3315
Policy version	3316
JSON policy document	3316
Learn more	3316
WAFLoggingServiceRolePolicy	3316
Using this policy	3317
Policy details	3317
Policy version	3317
JSON policy document	3317
Learn more	3318
WAFRegionalLoggingServiceRolePolicy	3318
Using this policy	3318
Policy details	3318
Policy version	3318
JSON policy document	3318
Learn more	3319
WAFV2LoggingServiceRolePolicy	3319
Using this policy	3319
Policy details	3319
Policy version	3320
JSON policy document	3320
Learn more	3320
WellArchitectedConsoleFullAccess	3321
Using this policy	3321
Policy details	3321
Policy version	3321
JSON policy document	3321
Learn more	3322
WellArchitectedConsoleReadOnlyAccess	3322
Using this policy	3322
Policy details	3322
Policy version	3322
JSON policy document	3322
Learn more	3323

WorkLinkServiceRolePolicy	3323
Using this policy	3323
Policy details	3323
Policy version	3324
JSON policy document	3324
Learn more	3324

What are AWS managed policies?

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases. They make it easier for you to get started with assigning permissions to users, groups, and roles than if you had to write the policies yourself.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they are available for use by all AWS customers. We recommend that you reduce permissions further by defining [customer managed policies](#) that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see [AWS managed policies](#) in the IAM User Guide.

Understanding policy reference pages

Each policy reference page includes the following information:

- **Using this policy** – Whether you can attach the policy to users, groups, and roles
- **Policy details**
 - **Type** – The type of AWS managed policy
 - **AWS managed policy** – A standard AWS managed policy
 - **Job function policy** – Policy that aligns with common industry job functions
 - **Service-linked role policy** – Policy that is attached to a service-linked role that allows a service to perform actions on your behalf, such as [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
 - **Service role policy** – Policy designed to work with service roles, such as [the section called “AWSControlTowerServiceRolePolicy”](#)
 - **Creation time** – When the policy was first created
 - **Edited time** – When this version of the policy was edited

- **ARN** – The Amazon Resource Name of the policy
- **Policy version** – The version of the permissions granted by the policy
- **JSON policy document** – The policy JSON
- **Learn more** – Links to documentation related to AWS managed policies

Deprecated AWS managed policies

AWS regularly updates AWS managed policies. In most cases, we add permissions to a policy. This happens when we launch a new service or feature. To improve the security of AWS managed policies, we sometimes reduce the scope of policies. When we remove permissions from a policy, we set the policy to a *deprecated* state and make a new one available. When AWS deprecates a service or feature, we also deprecate the AWS managed policy for that feature.

If you receive an email notification that a policy you are using is deprecated, we recommend that you immediately take action. Identify the change to the policy and update your workflows. If AWS provides a replacement policy, plan to attach it to all affected identities (users, groups, and roles) and then detach the deprecated policy from those identities.

A deprecated policy has the following characteristics:

- It is removed from this guide.
- Permissions continue to work for all *currently* attached identities.
- In accounts where the policy is attached to an identity, it appears in the **Policies** list in the IAM console with a warning icon next to it.
- It *cannot* be attached to any new identities. If you detach it from a current identity, you cannot reattach it.
- After you detach it from all current entities, it is no longer visible.

AWS managed policies

AWS managed policies

- [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](#)
- [AmazonCognitoIcmpEmailServiceRolePolicy](#)
- [AmazonCognitoIcmpServiceRolePolicy](#)
- [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](#)

- [AmazonElastiCacheReadOnlyAccess](#)
- [AmazonElasticContainerRegistryPublicFullAccess](#)
- [AmazonElasticContainerRegistryPublicPowerUser](#)
- [AmazonElasticContainerRegistryPublicReadOnly](#)
- [AmazonElasticFileSystemClientFullAccess](#)
- [AmazonElasticFileSystemClientReadOnlyAccess](#)
- [AmazonElasticFileSystemClientReadWriteAccess](#)
- [AmazonElasticFileSystemFullAccess](#)
- [AmazonElasticFileSystemReadOnlyAccess](#)
- [AmazonElasticFileSystemServiceRolePolicy](#)
- [AmazonElasticFileSystemsUtils](#)
- [AmazonElasticMapReduceEditorsRole](#)
- [AmazonElasticMapReduceforAutoScalingRole](#)
- [AmazonElasticMapReduceforEC2Role](#)
- [AmazonElasticMapReduceFullAccess](#)
- [AmazonElasticMapReducePlacementGroupPolicy](#)
- [AmazonElasticMapReduceReadOnlyAccess](#)
- [AmazonElasticMapReduceRole](#)
- [AmazonElasticsearchServiceRolePolicy](#)
- [AmazonElasticTranscoder_FullAccess](#)
- [AmazonElasticTranscoder_JobsSubmitter](#)
- [AmazonElasticTranscoder_ReadOnlyAccess](#)
- [AmazonElasticTranscoderRole](#)
- [AmazonEMRCleanupPolicy](#)
- [AmazonEMRContainersServiceRolePolicy](#)
- [AmazonEMRFullAccessPolicy_v2](#)
- [AmazonEMRReadOnlyAccessPolicy_v2](#)
- [AmazonEMRServerlessServiceRolePolicy](#)
- [AmazonEMRServicePolicy_v2](#)
- [AmazonESCognitoAccess](#)

- [AmazonESFullAccess](#)
- [AmazonESReadOnlyAccess](#)
- [AmazonEventBridgeApiDestinationsServiceRolePolicy](#)
- [AmazonEventBridgeFullAccess](#)
- [AmazonEventBridgePipesFullAccess](#)
- [AmazonEventBridgePipesOperatorAccess](#)
- [AmazonEventBridgePipesReadOnlyAccess](#)
- [AmazonEventBridgeReadOnlyAccess](#)
- [AmazonEventBridgeSchedulerFullAccess](#)
- [AmazonEventBridgeSchedulerReadOnlyAccess](#)
- [AmazonEventBridgeSchemasFullAccess](#)
- [AmazonEventBridgeSchemasReadOnlyAccess](#)
- [AmazonEventBridgeSchemasServiceRolePolicy](#)
- [AmazonFISServiceRolePolicy](#)
- [AmazonForecastFullAccess](#)
- [AmazonFraudDetectorFullAccessPolicy](#)
- [AmazonFreeRTOSFullAccess](#)
- [AmazonFreeRTOSOTAUpdate](#)
- [AmazonFSxConsoleFullAccess](#)
- [AmazonFSxConsoleReadOnlyAccess](#)
- [AmazonFSxFullAccess](#)
- [AmazonFSxReadOnlyAccess](#)
- [AmazonFSxServiceRolePolicy](#)
- [AmazonGlacierFullAccess](#)
- [AmazonGlacierReadOnlyAccess](#)
- [AmazonGrafanaAthenaAccess](#)
- [AmazonGrafanaCloudWatchAccess](#)
- [AmazonGrafanaRedshiftAccess](#)
- [AmazonGrafanaServiceLinkedRolePolicy](#)
- [AmazonGuardDutyFullAccess](#)

- [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#)
- [AmazonGuardDutyReadOnlyAccess](#)
- [AmazonGuardDutyServiceRolePolicy](#)
- [AmazonHealthLakeFullAccess](#)
- [AmazonHealthLakeReadOnlyAccess](#)
- [AmazonHoneycodeFullAccess](#)
- [AmazonHoneycodeReadOnlyAccess](#)
- [AmazonHoneycodeServiceRolePolicy](#)
- [AmazonHoneycodeTeamAssociationFullAccess](#)
- [AmazonHoneycodeTeamAssociationReadOnlyAccess](#)
- [AmazonHoneycodeWorkbookFullAccess](#)
- [AmazonHoneycodeWorkbookReadOnlyAccess](#)
- [AmazonInspector2AgentlessServiceRolePolicy](#)
- [AmazonInspector2FullAccess](#)
- [AmazonInspector2ManagedCisPolicy](#)
- [AmazonInspector2ReadOnlyAccess](#)
- [AmazonInspector2ServiceRolePolicy](#)
- [AmazonInspectorFullAccess](#)
- [AmazonInspectorReadOnlyAccess](#)
- [AmazonInspectorServiceRolePolicy](#)
- [AmazonKendraFullAccess](#)
- [AmazonKendraReadOnlyAccess](#)
- [AmazonKeyspacesFullAccess](#)
- [AmazonKeyspacesReadOnlyAccess](#)
- [AmazonKeyspacesReadOnlyAccess_v2](#)
- [AmazonKinesisAnalyticsFullAccess](#)
- [AmazonKinesisAnalyticsReadOnly](#)
- [AmazonKinesisFirehoseFullAccess](#)
- [AmazonKinesisFirehoseReadOnlyAccess](#)
- [AmazonKinesisFullAccess](#)

- [AmazonKinesisReadOnlyAccess](#)
- [AmazonKinesisVideoStreamsFullAccess](#)
- [AmazonKinesisVideoStreamsReadOnlyAccess](#)
- [AmazonLaunchWizard_Fullaccess](#)
- [AmazonLaunchWizardFullAccessV2](#)
- [AmazonLexChannelsAccess](#)
- [AmazonLexFullAccess](#)
- [AmazonLexReadOnly](#)
- [AmazonLexReplicationPolicy](#)
- [AmazonLexRunBotsOnly](#)
- [AmazonLexV2BotPolicy](#)
- [AmazonLookoutEquipmentFullAccess](#)
- [AmazonLookoutEquipmentReadOnlyAccess](#)
- [AmazonLookoutMetricsFullAccess](#)
- [AmazonLookoutMetricsReadOnlyAccess](#)
- [AmazonLookoutVisionConsoleFullAccess](#)
- [AmazonLookoutVisionConsoleReadOnlyAccess](#)
- [AmazonLookoutVisionFullAccess](#)
- [AmazonLookoutVisionReadOnlyAccess](#)
- [AmazonMachineLearningBatchPredictionsAccess](#)
- [AmazonMachineLearningCreateOnlyAccess](#)
- [AmazonMachineLearningFullAccess](#)
- [AmazonMachineLearningManageRealTimeEndpointOnlyAccess](#)
- [AmazonMachineLearningReadOnlyAccess](#)
- [AmazonMachineLearningRealTimePredictionOnlyAccess](#)
- [AmazonMachineLearningRoleforRedshiftDataSourceV3](#)
- [AmazonMacieFullAccess](#)
- [AmazonMacieHandshakeRole](#)
- [AmazonMacieReadOnlyAccess](#)
- [AmazonMacieServiceRole](#)

- [AmazonMacieServiceRolePolicy](#)
- [AmazonManagedBlockchainConsoleFullAccess](#)
- [AmazonManagedBlockchainFullAccess](#)
- [AmazonManagedBlockchainReadOnlyAccess](#)
- [AmazonManagedBlockchainServiceRolePolicy](#)
- [AmazonMCSFullAccess](#)
- [AmazonMCSReadOnlyAccess](#)
- [AmazonMechanicalTurkFullAccess](#)
- [AmazonMechanicalTurkReadOnly](#)
- [AmazonMemoryDBFullAccess](#)
- [AmazonMemoryDBReadOnlyAccess](#)
- [AmazonMobileAnalyticsFinancialReportAccess](#)
- [AmazonMobileAnalyticsFullAccess](#)
- [AmazonMobileAnalyticsNon-financialReportAccess](#)
- [AmazonMobileAnalyticsWriteOnlyAccess](#)
- [AmazonMonitronFullAccess](#)
- [AmazonMQApiFullAccess](#)
- [AmazonMQApiReadOnlyAccess](#)
- [AmazonMQFullAccess](#)
- [AmazonMQReadOnlyAccess](#)
- [AmazonMQServiceRolePolicy](#)
- [AmazonMSKConnectReadOnlyAccess](#)
- [AmazonMSKFullAccess](#)
- [AmazonMSKReadOnlyAccess](#)
- [AmazonMWAAServiceRolePolicy](#)
- [AmazonNimbleStudio-LaunchProfileWorker](#)
- [AmazonNimbleStudio-StudioAdmin](#)
- [AmazonNimbleStudio-StudioUser](#)
- [AmazonOmicsFullAccess](#)
- [AmazonOmicsReadOnlyAccess](#)

- [AmazonOneEnterpriseFullAccess](#)
- [AmazonOneEnterpriseInstallerAccess](#)
- [AmazonOneEnterpriseReadOnlyAccess](#)
- [AmazonOpenSearchDashboardsServiceRolePolicy](#)
- [AmazonOpenSearchDirectQueryGlueCreateAccess](#)
- [AmazonOpenSearchIngestionFullAccess](#)
- [AmazonOpenSearchIngestionReadOnlyAccess](#)
- [AmazonOpenSearchIngestionServiceRolePolicy](#)
- [AmazonOpenSearchServerlessServiceRolePolicy](#)
- [AmazonOpenSearchServiceCognitoAccess](#)
- [AmazonOpenSearchServiceFullAccess](#)
- [AmazonOpenSearchServiceReadOnlyAccess](#)
- [AmazonOpenSearchServiceRolePolicy](#)
- [AmazonPersonalizeFullAccess](#)
- [AmazonPollyFullAccess](#)
- [AmazonPollyReadOnlyAccess](#)
- [AmazonPrometheusConsoleFullAccess](#)
- [AmazonPrometheusFullAccess](#)
- [AmazonPrometheusQueryAccess](#)
- [AmazonPrometheusRemoteWriteAccess](#)
- [AmazonPrometheusScraperServiceRolePolicy](#)
- [AmazonQFullAccess](#)
- [AmazonQLDBConsoleFullAccess](#)
- [AmazonQLDBFullAccess](#)
- [AmazonQLDBReadOnly](#)
- [AmazonRDSBetaServiceRolePolicy](#)
- [AmazonRDSCustomInstanceProfileRolePolicy](#)
- [AmazonRDSCustomPreviewServiceRolePolicy](#)
- [AmazonRDSCustomServiceRolePolicy](#)
- [AmazonRDSDDataFullAccess](#)

- [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](#)
- [AmazonSSManagedEC2InstanceDefaultPolicy](#)
- [AmazonSSManagedInstanceCore](#)
- [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](#)
- [AmazonWorkSpacesPoolServiceAccess](#)
- [AmazonWorkSpacesSecureBrowserReadOnly](#)
- [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](#)
- [AWSApplicationAutoscalingWorkSpacesPoolPolicy](#)
- [AWSApplicationDiscoveryAgentAccess](#)
- [AWSApplicationDiscoveryAgentlessCollectorAccess](#)
- [AWSApplicationDiscoveryServiceFullAccess](#)
- [AWSApplicationMigrationAgentInstallationPolicy](#)
- [AWSApplicationMigrationAgentPolicy](#)
- [AWSApplicationMigrationAgentPolicy_v2](#)
- [AWSApplicationMigrationConversionServerPolicy](#)
- [AWSApplicationMigrationEC2Access](#)
- [AWSApplicationMigrationFullAccess](#)
- [AWSApplicationMigrationMGHAccess](#)
- [AWSApplicationMigrationReadOnlyAccess](#)
- [AWSApplicationMigrationReplicationServerPolicy](#)

- [AWSApplicationMigrationServiceEc2InstancePolicy](#)
- [AWSApplicationMigrationServiceRolePolicy](#)
- [AWSApplicationMigrationSSMAccess](#)
- [AWSApplicationMigrationVCenterClientPolicy](#)
- [AWSAppMeshEnvoyAccess](#)
- [AWSAppMeshFullAccess](#)
- [AWSAppMeshPreviewEnvoyAccess](#)
- [AWSAppMeshPreviewServiceRolePolicy](#)
- [AWSAppMeshReadOnly](#)
- [AWSAppMeshServiceRolePolicy](#)
- [AWSAppRunnerFullAccess](#)
- [AWSAppRunnerReadOnlyAccess](#)
- [AWSAppRunnerServicePolicyForECRAccess](#)
- [AWSAppSyncAdministrator](#)
- [AWSAppSyncInvokeFullAccess](#)
- [AWSAppSyncPushToCloudWatchLogs](#)
- [AWSAppSyncSchemaAuthor](#)
- [AWSAppSyncServiceRolePolicy](#)
- [AWSArtifactAccountSync](#)
- [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](#)
- [AWSCertificateManagerPrivateCAReadOnly](#)
- [AWSCertificateManagerPrivateCAUser](#)
- [AWSCertificateManagerReadOnly](#)
- [AWSChatbotServiceLinkedRolePolicy](#)
- [AWSCleanRoomsFullAccess](#)
- [AWSCleanRoomsFullAccessNoQuerying](#)

- [AWSCleanRoomsMLFullAccess](#)
- [AWSCleanRoomsMLReadOnlyAccess](#)
- [AWSCleanRoomsReadOnlyAccess](#)
- [AWSCloud9Administrator](#)
- [AWSCloud9EnvironmentMember](#)
- [AWSCloud9ServiceRolePolicy](#)
- [AWSCloud9SSMInstanceProfile](#)
- [AWSCloud9User](#)
- [AWSCloudFormationFullAccess](#)
- [AWSCloudFormationReadOnlyAccess](#)
- [AWSCloudFrontLogger](#)
- [AWSCloudHSMFullAccess](#)
- [AWSCloudHSMReadOnlyAccess](#)
- [AWSCloudHSMRole](#)
- [AWSCloudMapDiscoverInstanceAccess](#)
- [AWSCloudMapFullAccess](#)
- [AWSCloudMapReadOnlyAccess](#)
- [AWSCloudMapRegisterInstanceAccess](#)
- [AWSCloudShellFullAccess](#)
- [AWSCloudTrail_FullAccess](#)
- [AWSCloudTrail_ReadOnlyAccess](#)
- [AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy](#)
- [AWSCodeArtifactAdminAccess](#)
- [AWSCodeArtifactReadOnlyAccess](#)
- [AWSCodeBuildAdminAccess](#)
- [AWSCodeBuildDeveloperAccess](#)
- [AWSCodeBuildReadOnlyAccess](#)
- [AWSCodeCommitFullAccess](#)
- [AWSCodeCommitPowerUser](#)
- [AWSCodeCommitReadOnly](#)

- [AWSCodeDeployDeployerAccess](#)
- [AWSCodeDeployFullAccess](#)
- [AWSCodeDeployReadOnlyAccess](#)
- [AWSCodeDeployRole](#)
- [AWSCodeDeployRoleForCloudFormation](#)
- [AWSCodeDeployRoleForECS](#)
- [AWSCodeDeployRoleForECSLimited](#)
- [AWSCodeDeployRoleForLambda](#)
- [AWSCodeDeployRoleForLambdaLimited](#)
- [AWSCodePipeline_FullAccess](#)
- [AWSCodePipeline_ReadOnlyAccess](#)
- [AWSCodePipelineApproverAccess](#)
- [AWSCodePipelineCustomActionAccess](#)
- [AWSCodeStarFullAccess](#)
- [AWSCodeStarNotificationsServiceRolePolicy](#)
- [AWSCodeStarServiceRole](#)
- [AWSCompromisedKeyQuarantine](#)
- [AWSCompromisedKeyQuarantineV2](#)
- [AWSConfigMultiAccountSetupPolicy](#)
- [AWSConfigRemediationServiceRolePolicy](#)
- [AWSConfigRoleForOrganizations](#)
- [AWSConfigRulesExecutionRole](#)
- [AWSConfigServiceRolePolicy](#)
- [AWSConfigUserAccess](#)
- [AWSConnector](#)
- [AWSControlTowerAccountServiceRolePolicy](#)
- [AWSControlTowerServiceRolePolicy](#)
- [AWSCostAndUsageReportAutomationPolicy](#)
- [AWSDataExchangeFullAccess](#)
- [AWSDataExchangeProviderFullAccess](#)

- [AWSDataExchangeReadOnly](#)
- [AWSDataExchangeSubscriberFullAccess](#)
- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWSDataPipeline_FullAccess](#)
- [AWSDataPipeline_PowerUser](#)
- [AWSDataSyncDiscoveryServiceRolePolicy](#)
- [AWSDataSyncFullAccess](#)
- [AWSDataSyncReadOnlyAccess](#)
- [AWSDeadlineCloud-FleetWorker](#)
- [AWSDeadlineCloud-UserAccessFarms](#)
- [AWSDeadlineCloud-UserAccessFleets](#)
- [AWSDeadlineCloud-UserAccessJobs](#)
- [AWSDeadlineCloud-UserAccessQueues](#)
- [AWSDeadlineCloud-WorkerHost](#)
- [AWSDeepLensLambdaFunctionAccessPolicy](#)
- [AWSDeepLensServiceRolePolicy](#)
- [AWSDeepRacerAccountAdminAccess](#)
- [AWSDeepRacerCloudFormationAccessPolicy](#)
- [AWSDeepRacerDefaultMultiUserAccess](#)
- [AWSDeepRacerFullAccess](#)
- [AWSDeepRacerRoboMakerAccessPolicy](#)
- [AWSDeepRacerServiceRolePolicy](#)
- [AWSDenyAll](#)
- [AWSDeviceFarmFullAccess](#)
- [AWSDeviceFarmServiceRolePolicy](#)
- [AWSDeviceFarmTestGridServiceRolePolicy](#)
- [AWSDirectConnectFullAccess](#)
- [AWSDirectConnectReadOnlyAccess](#)

- [AWSDirectConnectServiceRolePolicy](#)
- [AWSDirectoryServiceFullAccess](#)
- [AWSDirectoryServiceReadOnlyAccess](#)
- [AWSDiscoveryContinuousExportFirehosePolicy](#)
- [AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWSDMSServerlessServiceRolePolicy](#)
- [AWSEC2CapacityReservationFleetRolePolicy](#)
- [AWSEC2FleetServiceRolePolicy](#)
- [AWSEC2SpotFleetServiceRolePolicy](#)
- [AWSEC2SpotServiceRolePolicy](#)
- [AWSEC2VssSnapshotPolicy](#)
- [AWSECRPullThroughCache_ServiceRolePolicy](#)
- [AWSElasticBeanstalkCustomPlatformforEC2Role](#)
- [AWSElasticBeanstalkEnhancedHealth](#)
- [AWSElasticBeanstalkMaintenance](#)
- [AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy](#)
- [AWSElasticBeanstalkManagedUpdatesServiceRolePolicy](#)
- [AWSElasticBeanstalkMulticontainerDocker](#)
- [AWSElasticBeanstalkReadOnly](#)
- [AWSElasticBeanstalkRoleCore](#)
- [AWSElasticBeanstalkRoleCWL](#)
- [AWSElasticBeanstalkRoleECS](#)
- [AWSElasticBeanstalkRoleRDS](#)
- [AWSElasticBeanstalkRoleSNS](#)
- [AWSElasticBeanstalkRoleWorkerTier](#)
- [AWSElasticBeanstalkService](#)
- [AWSElasticBeanstalkServiceRolePolicy](#)
- [AWSElasticBeanstalkWebTier](#)
- [AWSElasticBeanstalkWorkerTier](#)
- [AWSElasticDisasterRecoveryAgentInstallationPolicy](#)

- [AWSElasticDisasterRecoveryAgentPolicy](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess_v2](#)
- [AWSElasticDisasterRecoveryConversionServerPolicy](#)
- [AWSElasticDisasterRecoveryCrossAccountReplicationPolicy](#)
- [AWSElasticDisasterRecoveryEc2InstancePolicy](#)
- [AWSElasticDisasterRecoveryFailbackInstallationPolicy](#)
- [AWSElasticDisasterRecoveryFailbackPolicy](#)
- [AWSElasticDisasterRecoveryLaunchActionsPolicy](#)
- [AWSElasticDisasterRecoveryNetworkReplicationPolicy](#)
- [AWSElasticDisasterRecoveryReadOnlyAccess](#)
- [AWSElasticDisasterRecoveryRecoveryInstancePolicy](#)
- [AWSElasticDisasterRecoveryReplicationServerPolicy](#)
- [AWSElasticDisasterRecoveryServiceRolePolicy](#)
- [AWSElasticDisasterRecoveryStagingAccountPolicy](#)
- [AWSElasticDisasterRecoveryStagingAccountPolicy_v2](#)
- [AWSElasticLoadBalancingClassicServiceRolePolicy](#)
- [AWSElasticLoadBalancingServiceRolePolicy](#)
- [AWSElementalMediaConvertFullAccess](#)
- [AWSElementalMediaConvertReadOnly](#)
- [AWSElementalMediaLiveFullAccess](#)
- [AWSElementalMediaLiveReadOnly](#)
- [AWSElementalMediaPackageFullAccess](#)
- [AWSElementalMediaPackageReadOnly](#)
- [AWSElementalMediaPackageV2FullAccess](#)
- [AWSElementalMediaPackageV2ReadOnly](#)
- [AWSElementalMediaStoreFullAccess](#)
- [AWSElementalMediaStoreReadOnly](#)
- [AWSElementalMediaTailorFullAccess](#)
- [AWSElementalMediaTailorReadOnly](#)

- [AWSEnhancedClassicNetworkingMangementPolicy](#)
- [AWSEntityResolutionConsoleFullAccess](#)
- [AWSEntityResolutionConsoleReadOnlyAccess](#)
- [AWSFaultInjectionSimulatorEC2Access](#)
- [AWSFaultInjectionSimulatorECSAccess](#)
- [AWSFaultInjectionSimulatorEKSAccess](#)
- [AWSFaultInjectionSimulatorNetworkAccess](#)
- [AWSFaultInjectionSimulatorRDSAccess](#)
- [AWSFaultInjectionSimulatorSSMAccess](#)
- [AWSFinSpaceServiceRolePolicy](#)
- [AWSFMAdminFullAccess](#)
- [AWSFMAdminReadOnlyAccess](#)
- [AWSFMMemberReadOnlyAccess](#)
- [AWSForWordPressPluginPolicy](#)
- [AWSGitSyncServiceRolePolicy](#)
- [AWSGlobalAcceleratorSLRPolicy](#)
- [AWSGlueConsoleFullAccess](#)
- [AWSGlueConsoleSageMakerNotebookFullAccess](#)
- [AwsGlueDataBrewFullAccessPolicy](#)
- [AWSGlueDataBrewServiceRole](#)
- [AWSGlueSchemaRegistryFullAccess](#)
- [AWSGlueSchemaRegistryReadOnlyAccess](#)
- [AWSGlueServiceNotebookRole](#)
- [AWSGlueServiceRole](#)
- [AwsGlueSessionUserRestrictedNotebookPolicy](#)
- [AwsGlueSessionUserRestrictedNotebookServiceRole](#)
- [AwsGlueSessionUserRestrictedPolicy](#)
- [AwsGlueSessionUserRestrictedServiceRole](#)
- [AWSGrafanaAccountAdministrator](#)
- [AWSGrafanaConsoleReadOnlyAccess](#)

- [AWSGrafanaWorkspacePermissionManagement](#)
- [AWSGrafanaWorkspacePermissionManagementV2](#)
- [AWSGreengrassFullAccess](#)
- [AWSGreengrassReadOnlyAccess](#)
- [AWSGreengrassResourceAccessRolePolicy](#)
- [AWSGroundStationAgentInstancePolicy](#)
- [AWSHealth_EventProcessorServiceRolePolicy](#)
- [AWSHealthFullAccess](#)
- [AWSHealthImagingFullAccess](#)
- [AWSHealthImagingReadOnlyAccess](#)
- [AWSIAMIdentityCenterAllowListForIdentityContext](#)
- [AWSIdentitySyncFullAccess](#)
- [AWSIdentitySyncReadOnlyAccess](#)
- [AWSImageBuilderFullAccess](#)
- [AWSImageBuilderReadOnlyAccess](#)
- [AWSImportExportFullAccess](#)
- [AWSImportExportReadOnlyAccess](#)
- [AWSIncidentManagerIncidentAccessServiceRolePolicy](#)
- [AWSIncidentManagerResolverAccess](#)
- [AWSIncidentManagerServiceRolePolicy](#)
- [AWSIoTClickFullAccess](#)
- [AWSIoTClickReadOnlyAccess](#)
- [AWSIoTAnalyticsFullAccess](#)
- [AWSIoTAnalyticsReadOnlyAccess](#)
- [AWSIoTConfigAccess](#)
- [AWSIoTConfigReadOnlyAccess](#)
- [AWSIoTDataAccess](#)
- [AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction](#)
- [AWSIoTDeviceDefenderAudit](#)
- [AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction](#)

- [AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction](#)
- [AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateCACertMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction](#)
- [AWSIoTDeviceTesterForFreeRTOSFullAccess](#)
- [AWSIoTDeviceTesterForGreengrassFullAccess](#)
- [AWSIoTEventsFullAccess](#)
- [AWSIoTEventsReadOnlyAccess](#)
- [AWSIoTFleetHubFederationAccess](#)
- [AWSIoTFleetwiseServiceRolePolicy](#)
- [AWSIoTFullAccess](#)
- [AWSIoTLogging](#)
- [AWSIoTOTAUpdate](#)
- [AWSIoTRoboRunnerFullAccess](#)
- [AWSIoTRoboRunnerReadOnly](#)
- [AWSIoTRoboRunnerServiceRolePolicy](#)
- [AWSIoTRuleActions](#)
- [AWSIoTSiteWiseConsoleFullAccess](#)
- [AWSIoTSiteWiseFullAccess](#)
- [AWSIoTSiteWiseMonitorPortalAccess](#)
- [AWSIoTSiteWiseMonitorServiceRolePolicy](#)
- [AWSIoTSiteWiseReadOnlyAccess](#)
- [AWSIoTThingsRegistration](#)
- [AWSIoTTwinMakerServiceRolePolicy](#)
- [AWSIoTWirelessDataAccess](#)
- [AWSIoTWirelessFullAccess](#)
- [AWSIoTWirelessFullPublishAccess](#)
- [AWSIoTWirelessGatewayCertManager](#)
- [AWSIoTWirelessLogging](#)
- [AWSIoTWirelessReadOnlyAccess](#)

- [AWSIPAMServiceRolePolicy](#)
- [AWSIQContractServiceRolePolicy](#)
- [AWSIQFullAccess](#)
- [AWSIQPermissionServiceRolePolicy](#)
- [AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy](#)
- [AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy](#)
- [AWSKeyManagementServicePowerUser](#)
- [AWSLakeFormationCrossAccountManager](#)
- [AWSLakeFormationDataAdmin](#)
- [AWSLambda_FullAccess](#)
- [AWSLambda_ReadOnlyAccess](#)
- [AWSLambdaBasicExecutionRole](#)
- [AWSLambdaDynamoDBExecutionRole](#)
- [AWSLambdaENIManagementAccess](#)
- [AWSLambdaExecute](#)
- [AWSLambdaFullAccess](#)
- [AWSLambdaInvocation-DynamoDB](#)
- [AWSLambdaKinesisExecutionRole](#)
- [AWSLambdaMSKExecutionRole](#)
- [AWSLambdaReplicator](#)
- [AWSLambdaRole](#)
- [AWSLambdaSQSQueueExecutionRole](#)
- [AWSLambdaVPCAccessExecutionRole](#)
- [AWSLicenseManagerConsumptionPolicy](#)
- [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)
- [AWSLicenseManagerMasterAccountRolePolicy](#)
- [AWSLicenseManagerMemberAccountRolePolicy](#)
- [AWSLicenseManagerServiceRolePolicy](#)
- [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)
- [AWSM2ServicePolicy](#)

- [AWSManagedServices_ContactsServiceRolePolicy](#)
- [AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy](#)
- [AWSManagedServices_EventsServiceRolePolicy](#)
- [AWSManagedServicesDeploymentToolkitPolicy](#)
- [AWSMarketplaceAmiIngestion](#)
- [AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWSMarketplaceFullAccess](#)
- [AWSMarketplaceGetEntitlements](#)
- [AWSMarketplaceImageBuildFullAccess](#)
- [AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWSMarketplaceManageSubscriptions](#)
- [AWSMarketplaceMeteringFullAccess](#)
- [AWSMarketplaceMeteringRegisterUsage](#)
- [AWSMarketplaceProcurementSystemAdminFullAccess](#)
- [AWSMarketplacePurchaseOrdersServiceRolePolicy](#)
- [AWSMarketplaceRead-only](#)
- [AWSMarketplaceResaleAuthorizationServiceRolePolicy](#)
- [AWSMarketplaceSellerFullAccess](#)
- [AWSMarketplaceSellerProductsFullAccess](#)
- [AWSMarketplaceSellerProductsReadOnly](#)
- [AWSMediaConnectServicePolicy](#)
- [AWSMediaTailorServiceRolePolicy](#)
- [AWSMigrationHubDiscoveryAccess](#)
- [AWSMigrationHubDMSAccess](#)
- [AWSMigrationHubFullAccess](#)
- [AWSMigrationHubOrchestratorConsoleFullAccess](#)
- [AWSMigrationHubOrchestratorInstanceRolePolicy](#)
- [AWSMigrationHubOrchestratorPlugin](#)
- [AWSMigrationHubOrchestratorServiceRolePolicy](#)
- [AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess](#)

- [AWSMigrationHubRefactorSpaces-SSMAutomationPolicy](#)
- [AWSMigrationHubRefactorSpacesFullAccess](#)
- [AWSMigrationHubRefactorSpacesServiceRolePolicy](#)
- [AWSMigrationHubSMSAccess](#)
- [AWSMigrationHubStrategyCollector](#)
- [AWSMigrationHubStrategyConsoleFullAccess](#)
- [AWSMigrationHubStrategyServiceRolePolicy](#)
- [AWSMobileHub_FullAccess](#)
- [AWSMobileHub_ReadOnly](#)
- [AWSMSKReplicatorExecutionRole](#)
- [AWSNetworkFirewallServiceRolePolicy](#)
- [AWSNetworkManagerCloudWANServiceRolePolicy](#)
- [AWSNetworkManagerFullAccess](#)
- [AWSNetworkManagerReadOnlyAccess](#)
- [AWSNetworkManagerServiceRolePolicy](#)
- [AWSOpsWorks_FullAccess](#)
- [AWSOpsWorksCloudWatchLogs](#)
- [AWSOpsWorksCMInstanceProfileRole](#)
- [AWSOpsWorksCMServiceRole](#)
- [AWSOpsWorksInstanceRegistration](#)
- [AWSOpsWorksRegisterCLI_EC2](#)
- [AWSOpsWorksRegisterCLI_OnPremises](#)
- [AWSOrganizationsFullAccess](#)
- [AWSOrganizationsReadOnlyAccess](#)
- [AWSOrganizationsServiceTrustPolicy](#)
- [AWSOutpostsAuthorizeServerPolicy](#)
- [AWSOutpostsServiceRolePolicy](#)
- [AWSPanoramaApplianceRolePolicy](#)
- [AWSPanoramaApplianceServiceRolePolicy](#)
- [AWSPanoramaFullAccess](#)

- [AWSPanoramaGreengrassGroupRolePolicy](#)
- [AWSPanoramaSageMakerRolePolicy](#)
- [AWSPanoramaServiceLinkedRolePolicy](#)
- [AWSPanoramaServiceRolePolicy](#)
- [AWSPriceListServiceFullAccess](#)
- [AWSPrivateCAAuditor](#)
- [AWSPrivateCAFullAccess](#)
- [AWSPrivateCAPrivilegedUser](#)
- [AWSPrivateCARedOnly](#)
- [AWSPrivateCAUser](#)
- [AWSPrivateMarketplaceAdminFullAccess](#)
- [AWSPrivateMarketplaceRequests](#)
- [AWSPrivateNetworksServiceRolePolicy](#)
- [AWSProtonCodeBuildProvisioningBasicAccess](#)
- [AWSProtonCodeBuildProvisioningServiceRolePolicy](#)
- [AWSProtonDeveloperAccess](#)
- [AWSProtonFullAccess](#)
- [AWSProtonReadOnlyAccess](#)
- [AWSProtonServiceGitSyncServiceRolePolicy](#)
- [AWSProtonSyncServiceRolePolicy](#)
- [AWSPurchaseOrdersServiceRolePolicy](#)
- [AWSQuickSetupCFGCPacksPermissionsBoundary](#)
- [AWSQuickSetupDeploymentRolePolicy](#)
- [AWSQuickSetupDevOpsGuruPermissionsBoundary](#)
- [AWSQuickSetupDistributorPermissionsBoundary](#)
- [AWSQuickSetupPatchPolicyBaselineAccess](#)
- [AWSQuickSetupPatchPolicyDeploymentRolePolicy](#)
- [AWSQuickSetupPatchPolicyPermissionsBoundary](#)
- [AWSQuickSetupSchedulerPermissionsBoundary](#)
- [AWSQuickSetupSSMHostMgmtPermissionsBoundary](#)

- [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](#)
- [AWSSStepFunctionsConsoleFullAccess](#)
- [AWSSStepFunctionsFullAccess](#)
- [AWSSStepFunctionsReadOnlyAccess](#)
- [AWSSStorageGatewayFullAccess](#)
- [AWSSStorageGatewayReadOnlyAccess](#)
- [AWSSStorageGatewayServiceRolePolicy](#)
- [AWSSSupplyChainFederationAdminAccess](#)
- [AWSSupportAccess](#)
- [AWSSupportAppFullAccess](#)
- [AWSSupportAppReadOnlyAccess](#)
- [AWSSupportPlansFullAccess](#)
- [AWSSupportPlansReadOnlyAccess](#)
- [AWSSupportServiceRolePolicy](#)
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSSystemsManagerChangeManagementServicePolicy](#)

- [AWSSystemsManagerEnableConfigRecordingExecutionPolicy](#)
- [AWSSystemsManagerEnableExplorerExecutionPolicy](#)
- [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](#)
- [ECRTemplateServiceRolePolicy](#)
- [ElastiCacheServiceRolePolicy](#)
- [ElasticLoadBalancingFullAccess](#)
- [ElasticLoadBalancingReadOnly](#)
- [ElementalActivationsDownloadSoftwareAccess](#)
- [ElementalActivationsFullAccess](#)
- [ElementalActivationsGenerateLicenses](#)
- [ElementalActivationsReadOnlyAccess](#)
- [ElementalAppliancesSoftwareFullAccess](#)

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

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

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

Description: Allow Access Analyzer to analyze resource metadata

AccessAnalyzerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 02, 2019, 17:13 UTC
- **Edited time:** May 30, 2024, 18:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Policy version

Policy version: v13 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AdministratorAccess

Description: Provides full access to AWS services and resources.

AdministratorAccess is an [AWS managed policy](#).

Using this policy

You can attach AdministratorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** February 06, 2015, 18:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AdministratorAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AdministratorAccess-Amplify

Description: Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applications.

AdministratorAccess-Amplify is an [AWS managed policy](#).

Using this policy

You can attach AdministratorAccess-Amplify to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 19:03 UTC
- **Edited time:** April 04, 2024, 20:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AdministratorAccess-Amplify

Policy version

Policy version: v12 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AdministratorAccess-AWSElasticBeanstalk

Description: Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to resources they need to manage AWS Elastic Beanstalk applications

AdministratorAccess-AWSElasticBeanstalk is an [AWS managed policy](#).

Using this policy

You can attach AdministratorAccess-AWSElasticBeanstalk to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 22, 2021, 19:36 UTC
- **Edited time:** March 23, 2023, 23:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
"sq: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"
      ]
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessDeviceSetup

Description: Provide device setup access to AlexaForBusiness services

AlexaForBusinessDeviceSetup is an [AWS managed policy](#).

Using this policy

You can attach AlexaForBusinessDeviceSetup to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:47 UTC
- **Edited time:** May 20, 2019, 21:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessFullAccess

Description: Grants full access to AlexaForBusiness resources and access to related AWS services

AlexaForBusinessFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AlexaForBusinessFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** November 30, 2017, 16:47 UTC
- **Edited time:** July 01, 2020, 21:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessGatewayExecution

Description: Provide gateway execution access to AlexaForBusiness services

AlexaForBusinessGatewayExecution is an [AWS managed policy](#).

Using this policy

You can attach `AlexaForBusinessGatewayExecution` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:47 UTC
- **Edited time:** November 30, 2017, 16:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

Description: Provide access to Lifesize AVS devices

AlexaForBusinessLifesizeDelegatedAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AlexaForBusinessLifesizeDelegatedAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 04, 2020, 19:46 UTC

- **Edited time:** June 12, 2020, 20:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

```
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b>DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b>DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
    ],
    "Resource" : "*"
},
{
    "Action" : [
        "kms:DescribeKey"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:kms:*:*:key/*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessNetworkProfileServicePolicy

Description: This policy enables Alexa for Business to perform automated tasks scheduled by your network profiles.

AlexaForBusinessNetworkProfileServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 13, 2019, 00:53 UTC
- **Edited time:** April 05, 2019, 21:57 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessPolyDelegatedAccessPolicy

Description: Provide access to Poly AVS devices

AlexaForBusinessPolyDelegatedAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AlexaForBusinessPolyDelegatedAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 16, 2019, 19:48 UTC
- **Edited time:** October 16, 2019, 19:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AlexaForBusinessReadOnlyAccess

Description: Provide read only access to AlexaForBusiness services

AlexaForBusinessReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AlexaForBusinessReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:47 UTC
- **Edited time:** November 20, 2019, 00:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAPIGatewayAdministrator

Description: Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.

AmazonAPIGatewayAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AmazonAPIGatewayAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:34 UTC
- **Edited time:** July 09, 2015, 17:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAPIGatewayInvokeFullAccess

Description: Provides full access to invoke APIs in Amazon API Gateway.

AmazonAPIGatewayInvokeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAPIGatewayInvokeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:36 UTC
- **Edited time:** December 18, 2018, 18:25 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAPIGatewayPushToCloudWatchLogs

Description: Allows API Gateway to push logs to user's account.

AmazonAPIGatewayPushToCloudWatchLogs is an [AWS managed policy](#).

Using this policy

You can attach AmazonAPIGatewayPushToCloudWatchLogs to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 11, 2015, 23:41 UTC
- **Edited time:** November 11, 2015, 23:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppFlowFullAccess

Description: Provides full access to Amazon AppFlow and access to AWS services supported as flow source or destination (S3 and Redshift). Also provides access to KMS for encryption

AmazonAppFlowFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAppFlowFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 02, 2020, 23:30 UTC
- **Edited time:** February 28, 2022, 23:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppFlowReadOnlyAccess

Description: Provides read only access to Amazon Appflow flows

AmazonAppFlowReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAppFlowReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 02, 2020, 23:26 UTC
- **Edited time:** February 28, 2022, 20:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppStreamFullAccess

Description: Provides full access to Amazon AppStream via the AWS Management Console.

AmazonAppStreamFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAppStreamFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** August 28, 2020, 17:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppStreamPCAAccess

Description: Amazon AppStream 2.0 access to AWS Certificate Manager Private CA in customer accounts for certificate-based authentication

AmazonAppStreamPCAAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAppStreamPCAAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 24, 2022, 17:05 UTC
- **Edited time:** October 24, 2022, 17:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppStreamReadOnlyAccess

Description: Provides read only access to Amazon AppStream via the AWS Management Console.

AmazonAppStreamReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAppStreamReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** December 07, 2016, 21:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAppStreamServiceAccess

Description: Default policy for Amazon AppStream service role.

AmazonAppStreamServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonAppStreamServiceAccess` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 19, 2016, 04:17 UTC
- **Edited time:** June 26, 2020, 16:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAthenaFullAccess

Description: Provide full access to Amazon Athena and scoped access to the dependencies needed to enable querying, writing results, and data management.

AmazonAthenaFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonAthenaFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2016, 16:46 UTC
- **Edited time:** June 20, 2024, 16:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Policy version

Policy version: v12 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
    "glue:GetCatalogImportStatus"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseQueryResultsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:PutObject",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-athena-query-results-*"
  ]
},
```

```
{
  "Sid" : "BaseAthenaExamplesPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::athena-examples*"
  ]
},
{
  "Sid" : "BaseS3BucketPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseSNSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:GetTopicAttributes"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseCloudWatchPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "BaseLakeFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "lakeformation:GetDataAccess"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "BaseDataZonePermissions",
    "Effect" : "Allow",
    "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "BasePricingPermissions",
    "Effect" : "Allow",
    "Action" : [
        "pricing:GetProducts"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAugmentedAIFullAccess

Description: Provides access to perform all operations Amazon Augmented AI resources, including FlowDefinitions, HumanTaskUis and HumanLoops. Does not allow access for creating FlowDefinitions against the public-crowd Workteam.

AmazonAugmentedAIFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAugmentedAIFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 16:21 UTC
- **Edited time:** December 03, 2019, 16:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAugmentedAIHumanLoopFullAccess

Description: Provides access to perform all operations on HumanLoops.

AmazonAugmentedAIHumanLoopFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAugmentedAIHumanLoopFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 16:20 UTC
- **Edited time:** December 03, 2019, 16:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonAugmentedAIIntegratedAPIAccess

Description: Provides access to perform all operations Amazon Augmented AI resources, including FlowDefinitions, HumanTaskUis and HumanLoops. Also provides access to those operations of services that are integrated with Amazon Augmented AI.

AmazonAugmentedAIIntegratedAPIAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonAugmentedAIIntegratedAPIAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 22, 2020, 20:47 UTC
- **Edited time:** April 22, 2020, 20:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonBedrockFullAccess

Description: Provides full access to Amazon Bedrock as well as limited access to related services that are required by it

AmazonBedrockFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonBedrockFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 06, 2023, 15:47 UTC
- **Edited time:** December 06, 2023, 15:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonBedrockFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonBedrockReadOnly

Description: Provides read only access to Amazon Bedrock

AmazonBedrockReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonBedrockReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 06, 2023, 15:48 UTC
- **Edited time:** December 06, 2023, 15:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonBedrockReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonBraketFullAccess

Description: Provides full access to Amazon Braket via the AWS Management Console and SDK. Also provides access to related services (e.g., S3, logs).

AmazonBraketFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonBraketFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 06, 2020, 20:12 UTC
- **Edited time:** April 19, 2023, 16:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonBraketJobsExecutionPolicy

Description: Grants access to AWS services and resources necessary for executing an Amazon Braket Job including S3, Cloudwatch, IAM and Braket

AmazonBraketJobsExecutionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonBraketJobsExecutionPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 26, 2021, 19:34 UTC
- **Edited time:** November 28, 2021, 05:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
} ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonBraketServiceRolePolicy

Description: Allows Amazon Braket to create and manage AWS resources on your behalf

AmazonBraketServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 04, 2020, 17:12 UTC
- **Edited time:** August 06, 2020, 20:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeFullAccess

Description: Provides full access to Amazon Chime Admin Console via the AWS Management Console.

AmazonChimeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonChimeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 01, 2017, 22:15 UTC
- **Edited time:** December 14, 2020, 21:00 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeReadOnly

Description: Provides read only access to Amazon Chime Admin Console via the AWS Management Console.

AmazonChimeReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonChimeReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 01, 2017, 22:04 UTC
- **Edited time:** December 14, 2020, 20:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonChimeReadOnly

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeSDK

Description: Provides access to Amazon Chime SDK operations

AmazonChimeSDK is an [AWS managed policy](#).

Using this policy

You can attach AmazonChimeSDK to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 04, 2020, 21:53 UTC
- **Edited time:** January 10, 2023, 18:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonChimeSDK

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Description: Managed Policy For Amazon Chime SDK MediaPipelines Service Linked Role

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 04, 2022, 22:02 UTC
- **Edited time:** December 08, 2023, 19:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeSDKMessagingServiceRolePolicy

Description: Allows Amazon Chime SDK Messaging to access AWS resources and enable messaging functionality

AmazonChimeSDKMessagingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 03, 2023, 01:43 UTC
- **Edited time:** March 03, 2023, 01:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeServiceRolePolicy

Description: Enables access to AWS Resources used or managed by Amazon Chime

AmazonChimeServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 30, 2019, 22:25 UTC
- **Edited time:** September 30, 2019, 22:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

Description: Allows Amazon Chime to access Amazon Transcribe and Amazon Transcribe Medical on your behalf

AmazonChimeTranscriptionServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 04, 2021, 21:47 UTC
- **Edited time:** August 04, 2021, 21:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeUserManagement

Description: Provides user management access to Amazon Chime Admin Console via the AWS Management Console.

AmazonChimeUserManagement is an [AWS managed policy](#).

Using this policy

You can attach AmazonChimeUserManagement to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 01, 2017, 22:17 UTC
- **Edited time:** February 18, 2020, 19:26 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonChimeUserManagement

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Description: Managed policy for Service Linked Role for Amazon Chime VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 30, 2019, 22:16 UTC

- **Edited time:** April 14, 2023, 21:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudDirectoryFullAccess

Description: Provides full access to Amazon Cloud Directory Service.

AmazonCloudDirectoryFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudDirectoryFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 25, 2017, 00:41 UTC
- **Edited time:** February 25, 2017, 00:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudDirectoryReadOnlyAccess

Description: Provides read only access to Amazon Cloud Directory Service.

AmazonCloudDirectoryReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudDirectoryReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 28, 2017, 23:42 UTC
- **Edited time:** February 28, 2017, 23:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchEvidentlyFullAccess

Description: Provides full only access to Amazon CloudWatch Evidently. Also provides access to related Amazon S3, Amazon SNS, Amazon CloudWatch, and other related services.

AmazonCloudWatchEvidentlyFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudWatchEvidentlyFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 15:10 UTC
- **Edited time:** November 29, 2021, 15:10 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

Description: Provides read only access to Amazon CloudWatch Evidently

AmazonCloudWatchEvidentlyReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudWatchEvidentlyReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 15:08 UTC
- **Edited time:** November 29, 2021, 15:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

Description: Allows CloudWatch Evidently Service to manage associated AWS Resources on behalf of the customer

AmazonCloudWatchEvidentlyServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** September 13, 2022, 17:25 UTC
- **Edited time:** September 13, 2022, 17:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchRUMFullAccess

Description: Grants full access permissions for the Amazon CloudWatch RUM service

AmazonCloudWatchRUMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudWatchRUMFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 15:46 UTC
- **Edited time:** November 29, 2021, 15:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchRUMReadOnlyAccess

Description: Grants read only permissions for the Amazon CloudWatch RUM service

AmazonCloudWatchRUMReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCloudWatchRUMReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 15:43 UTC
- **Edited time:** October 28, 2022, 18:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCloudWatchRUMServiceRolePolicy

Description: Grants permission to Amazon CloudWatch RUM Service to publish monitoring data to other relevant AWS services

AmazonCloudWatchRUMServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 17, 2021, 23:17 UTC

- **Edited time:** February 22, 2023, 20:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeCatalystFullAccess

Description: Provides full access to Amazon CodeCatalyst

AmazonCodeCatalystFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeCatalystFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 20, 2023, 16:50 UTC
- **Edited time:** April 20, 2023, 16:50 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeCatalystReadOnlyAccess

Description: Provides read only access to Amazon CodeCatalyst

AmazonCodeCatalystReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeCatalystReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 20, 2023, 16:49 UTC
- **Edited time:** April 20, 2023, 16:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeCatalystSupportAccess

Description: Allows Amazon CodeCatalyst to create, update, and resolve AWS Support cases on your behalf.

AmazonCodeCatalystSupportAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeCatalystSupportAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2023, 12:34 UTC
- **Edited time:** April 20, 2023, 12:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruProfilerAgentAccess

Description: Provides access required by Amazon CodeGuru Profiler agent.

AmazonCodeGuruProfilerAgentAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeGuruProfilerAgentAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 05, 2021, 22:11 UTC
- **Edited time:** May 05, 2022, 18:11 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruProfilerFullAccess

Description: Provides full access to Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonCodeGuruProfilerFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 10:13 UTC
- **Edited time:** July 15, 2020, 03:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruProfilerReadOnlyAccess

Description: Provides read only access to Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeGuruProfilerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 10:30 UTC
- **Edited time:** June 27, 2020, 23:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruReviewerFullAccess

Description: Grants full access to Amazon CodeGuru Reviewer and scoped access to required dependencies.

AmazonCodeGuruReviewerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonCodeGuruReviewerFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 08:33 UTC
- **Edited time:** August 29, 2020, 04:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruReviewerReadOnlyAccess

Description: Provides read only access to Amazon CodeGuru Reviewer.

AmazonCodeGuruReviewerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeGuruReviewerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 08:48 UTC
- **Edited time:** August 29, 2020, 04:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruReviewerServiceRolePolicy

Description: A service-linked role required for Amazon CodeGuru Reviewer to access resources on your behalf.

AmazonCodeGuruReviewerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 03, 2019, 05:31 UTC

- **Edited time:** November 27, 2020, 15:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruSecurityFullAccess

Description: Provides full access to Amazon CodeGuru Security.

AmazonCodeGuruSecurityFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeGuruSecurityFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2023, 21:03 UTC
- **Edited time:** May 09, 2023, 21:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCodeGuruSecurityScanAccess

Description: Provides access required for working with Amazon CodeGuru Security scans.

AmazonCodeGuruSecurityScanAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonCodeGuruSecurityScanAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2023, 20:54 UTC
- **Edited time:** May 09, 2023, 20:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoDeveloperAuthenticatedIdentities

Description: Provides access to Amazon Cognito APIs to support developer authenticated identities from your authentication backend.

AmazonCognitoDeveloperAuthenticatedIdentities is an [AWS managed policy](#).

Using this policy

You can attach AmazonCognitoDeveloperAuthenticatedIdentities to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 24, 2015, 17:22 UTC
- **Edited time:** March 24, 2015, 17:22 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Effect" : "Allow",
"Action" : [
  "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
  "cognito-identity:LookupDeveloperIdentity",
  "cognito-identity:MergeDeveloperIdentities",
  "cognito-identity:UnlinkDeveloperIdentity"
],
"Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoIdpEmailServiceRolePolicy

Description: Allows Amazon Cognito User Pools service to use your SES identities for email sending

AmazonCognitoIdpEmailServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 21, 2019, 21:32 UTC
- **Edited time:** March 21, 2019, 21:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoIdpServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Amazon Cognito User Pools

AmazonCognitoIdpServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 26, 2020, 22:30 UTC
- **Edited time:** June 26, 2020, 22:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoPowerUser

Description: Provides administrative access to existing Amazon Cognito resources. You will need AWS account admin privileges to create new Cognito resources.

AmazonCognitoPowerUser is an [AWS managed policy](#).

Using this policy

You can attach AmazonCognitoPowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 24, 2015, 17:14 UTC
- **Edited time:** June 01, 2021, 17:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCognitoPowerUser

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoReadOnly

Description: Provides read only access to Amazon Cognito resources.

AmazonCognitoReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonCognitoReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 24, 2015, 17:06 UTC
- **Edited time:** August 01, 2019, 19:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCognitoReadOnly

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Description: This policy defines the set of permissions allowed for unauthenticated identities for Cognito Identity Pools. This policy is not intended to be used as a stand alone permission policy.

It is used as a guardrail against overly permissive policies attached for roles in an identity pool. Do not attach this policy to any roles, as Cognito Identity Service will automatically include it as a scoped down policy when creating credentials. The privileges to temporarily access other AWS resources through the enhanced flow will now be defined by the intersection of the role associated with the identity of the unauthenticated user provided by a service, and the privileges given in this managed policy that is owned by Cognito.

AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 19, 2023, 23:04 UTC
- **Edited time:** July 19, 2023, 23:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonCognitoUnauthenticatedIdentities

Description: This policy defines the set of permissions allowed for unauthenticated identities for Cognito Identity Pools. This does not need to be attached to your unauth role, as Cognito Identity Service will automatically include it as a scoped down policy when creating credentials. The privileges to temporarily access other AWS resources through the enhanced flow will now be defined by the intersection of the role associated with the identity of the unauthenticated user provided by a service, and the privileges given in this managed policy that is owned by Cognito.

AmazonCognitoUnauthenticatedIdentities is an [AWS managed policy](#).

Using this policy

You can attach AmazonCognitoUnauthenticatedIdentities to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 01, 2023, 22:36 UTC
- **Edited time:** February 01, 2023, 22:36 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnect_FullAccess

Description: The purpose of this policy is to grant permissions to AWS Connect users required to use Connect resources. This policy provides full access to AWS Connect resources via the Connect Console and public APIs

AmazonConnect_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonConnect_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 20, 2020, 19:54 UTC
- **Edited time:** March 07, 2023, 14:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonConnect_FullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
    }
}

```

```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

Description: Policy for Amazon Connect Campaigns service linked role

AmazonConnectCampaignsServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 23, 2021, 20:54 UTC
- **Edited time:** November 08, 2023, 16:16 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnectReadOnlyAccess

Description: Grants permission to view the Amazon Connect instances in your AWS account.

AmazonConnectReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonConnectReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 17, 2018, 21:00 UTC
- **Edited time:** June 19, 2024, 15:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnectServiceLinkedRolePolicy

Description: Allows Amazon Connect to create and manage AWS resources on your behalf.

AmazonConnectServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 07, 2018, 00:21 UTC
- **Edited time:** May 24, 2024, 01:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Policy version

Policy version: v16 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```

"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/*"
    ]
  }
]

```

```
}  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnectSynchronizationServiceRolePolicy

Description: Allows Amazon Connect to synchronize AWS resources across regions on your behalf.

AmazonConnectSynchronizationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 27, 2023, 22:38 UTC
- **Edited time:** October 27, 2023, 22:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonConnectVoiceIDFullAccess

Description: Provides full access to Amazon Connect Voice ID

AmazonConnectVoiceIDFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonConnectVoiceIDFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 26, 2021, 19:04 UTC
- **Edited time:** September 26, 2021, 19:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneDomainExecutionRolePolicy

Description: Default policy for the Amazon DataZone's DomainExecutionRole service role. This role is used by Amazon DataZone to catalog, discover, govern, share, and analyze data in the Amazon DataZone domain.

AmazonDataZoneDomainExecutionRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneDomainExecutionRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 27, 2023, 21:55 UTC
- **Edited time:** June 27, 2024, 15:17 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
    "datazone:GetEnvironmentAction",
    "datazone:ListEnvironmentActions",
    "datazone:ListLineageNodeHistory",
    "datazone:GetLineageNode",
    "datazone:CreateAssetFilter",
    "datazone>DeleteAssetFilter",
    "datazone:GetAssetFilter",
    "datazone:ListAssetFilters",
    "datazone:UpdateAssetFilter"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RAMResourceShareStatement",
  "Effect" : "Allow",
  "Action" : "ram:GetResourceShareAssociations",
  "Resource" : "*"
}

```

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

Description: Amazon DataZone creates IAM roles for Environments to perform data analytics actions, and uses this policy when creating these roles to define the boundary of their permissions.

AmazonDataZoneEnvironmentRolePermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneEnvironmentRolePermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 11, 2023, 23:38 UTC
- **Edited time:** November 17, 2023, 23:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneFullAccess

Description: Provides full access to Amazon DataZone via the AWS Management Console as well as limited access to related services that are required by it.

AmazonDataZoneFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 22, 2023, 20:06 UTC
- **Edited time:** June 13, 2024, 19:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

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

```

```

    "StringEqualsIfExists" : {
      "ram:RequestedResourceType" : "datazone:Domain"
    }
  },
  {
    "Sid" : "RamResourceStatement",
    "Effect" : "Allow",
    "Action" : [
      "ram:DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:RejectResourceShareInvitation"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : [
          "DataZone*"
        ]
      }
    }
  },
  {
    "Sid" : "RamResourceReadOnlyStatement",
    "Effect" : "Allow",
    "Action" : [
      "ram:GetResourceShares",
      "ram:GetResourceShareInvitations",
      "ram:GetResourceShareAssociations",
      "ram:ListResourceSharePermissions"
    ],
    "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" : "DataZoneTagOnCreateDomainProjectTags",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:AmazonDataZone-*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneDomain",
                "AmazonDataZoneProject"
            ]
        },
        "StringLike" : {
            "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
            "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*"
        }
    }
},
{
    "Sid" : "DataZoneTagOnCreate",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:AmazonDataZone-*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneDomain"
            ]
        }
    ]
}
```

```

    },
    "StringLike" : {
      "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
      "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*"
    }
  }
},
{
  "Sid" : "CreateSecretStatement",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneFullUserAccess

Description: Provides full access to Amazon DataZone, but does not allow the management of domains, users, or associated accounts.

AmazonDataZoneFullUserAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneFullUserAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 22, 2023, 21:06 UTC
- **Edited time:** June 27, 2024, 15:18 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:ListGroupsWithUser",
        "datazone>DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",

```

```
"datazone:DeleteAssetType",
"datazone:CreateGlossary",
"datazone:GetGlossary",
"datazone:DeleteGlossary",
"datazone:UpdateGlossary",
"datazone:CreateGlossaryTerm",
"datazone:GetGlossaryTerm",
"datazone:DeleteGlossaryTerm",
"datazone:UpdateGlossaryTerm",
"datazone:CreateAsset",
"datazone:GetAsset",
"datazone:DeleteAsset",
"datazone:CreateAssetRevision",
"datazone:ListAssetRevisions",
"datazone:AcceptPredictions",
"datazone:RejectPredictions",
"datazone:Search",
"datazone:SearchTypes",
"datazone:CreateListingChangeSet",
"datazone:DeleteListing",
"datazone:SearchListings",
"datazone:GetListing",
"datazone:CreateDataSource",
"datazone:GetDataSource",
"datazone:DeleteDataSource",
"datazone:UpdateDataSource",
"datazone:ListDataSources",
"datazone:StartDataSourceRun",
"datazone:GetDataSourceRun",
"datazone:ListDataSourceRuns",
"datazone:ListDataSourceRunActivities",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:CreateEnvironmentBlueprint",
"datazone:GetEnvironmentBlueprint",
"datazone:DeleteEnvironmentBlueprint",
"datazone:UpdateEnvironmentBlueprint",
"datazone:ListEnvironmentBlueprints",
"datazone:CreateProject",
"datazone:UpdateProject",
"datazone:GetProject",
"datazone:DeleteProject",
"datazone:ListProjects",
"datazone:CreateProjectMembership",
"datazone:DeleteProjectMembership",
```



```
"datazone:ListProjectMemberships",
"datazone:CreateEnvironmentProfile",
"datazone:GetEnvironmentProfile",
"datazone:UpdateEnvironmentProfile",
"datazone>DeleteEnvironmentProfile",
"datazone:ListEnvironmentProfiles",
"datazone:CreateEnvironment",
"datazone:GetEnvironment",
"datazone>DeleteEnvironment",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:ListEnvironments",
"datazone:ListAccountEnvironments",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentCredentials",
"datazone:GetSubscriptionTarget",
"datazone>DeleteSubscriptionTarget",
"datazone:ListSubscriptionTargets",
"datazone:CreateSubscriptionRequest",
"datazone:AcceptSubscriptionRequest",
"datazone:UpdateSubscriptionRequest",
"datazone:ListWarehouseMetadata",
"datazone:RejectSubscriptionRequest",
"datazone:GetSubscriptionRequestDetails",
"datazone:ListSubscriptionRequests",
"datazone>DeleteSubscriptionRequest",
"datazone:GetSubscription",
"datazone:CancelSubscription",
"datazone:GetSubscriptionEligibility",
"datazone:ListSubscriptions",
"datazone:RevokeSubscription",
"datazone:CreateSubscriptionGrant",
"datazone>DeleteSubscriptionGrant",
"datazone:GetSubscriptionGrant",
"datazone:ListSubscriptionGrants",
"datazone:UpdateSubscriptionGrantStatus",
"datazone:ListNotifications",
"datazone:StartMetadataGenerationRun",
"datazone:GetMetadataGenerationRun",
"datazone:CancelMetadataGenerationRun",
"datazone:ListMetadataGenerationRuns",
"datazone:ListLineageNodeHistory",
"datazone:GetLineageNode",
"datazone:CreateAssetFilter",
```

```
        "datazone:DeleteAssetFilter",
        "datazone:GetAssetFilter",
        "datazone:ListAssetFilters",
        "datazone:UpdateAssetFilter"
    ],
    "Resource" : "*"
},
{
    "Sid" : "RAMResourceShareOperations",
    "Effect" : "Allow",
    "Action" : "ram:GetResourceShareAssociations",
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneGlueManageAccessRolePolicy

Description: The policy grants permissions to allow Amazon DataZone to enable publishing and access grants to data.

AmazonDataZoneGlueManageAccessRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneGlueManageAccessRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 22, 2023, 20:21 UTC

- **Edited time:** June 28, 2024, 16:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:CreateDataCellsFilter",
      "lakeformation:CreateLakeFormationOptIn",
      "lakeformation>DeleteDataCellsFilter",
      "lakeformation>DeleteLakeFormationOptIn",
      "lakeformation:GrantPermissions",
      "lakeformation:GetDataCellsFilter",
      "lakeformation:GetResourceLFTags",
      "lakeformation:ListDataCellsFilter",
      "lakeformation:ListLakeFormationOptIns",
      "lakeformation:ListPermissions",
```

```

        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
    ],
    "Resource" : "*"
},
{
    "Sid" : "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"
    ]
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZonePortalFullAccessPolicy

Description: Provides full access to Amazon DataZone APIs

AmazonDataZonePortalFullAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZonePortalFullAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 26, 2023, 18:24 UTC
- **Edited time:** March 26, 2023, 18:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZonePreviewConsoleFullAccess

Description: Provides full access to the Preview release of Amazon DataZone via the AWS Management Console. Also provides select access to other related services.

AmazonDataZonePreviewConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZonePreviewConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 28, 2023, 15:16 UTC
- **Edited time:** July 13, 2023, 18:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

Description: Amazon DataZone creates IAM roles that it uses for deploying data analytics projects. DataZone uses this policy when creating these roles to define the boundary of their permissions.

AmazonDataZoneProjectDeploymentPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneProjectDeploymentPermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 21, 2023, 02:54 UTC
- **Edited time:** April 04, 2023, 02:48 UTC
- **ARN:** arn:aws:iam::aws:policy/
AmazonDataZoneProjectDeploymentPermissionsBoundary

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    ]
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneProjectRolePermissionsBoundary

Description: Amazon DataZone creates IAM roles for projects to perform data analytics actions, and uses this policy when creating these roles to define the boundary of their permissions.

AmazonDataZoneProjectRolePermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneProjectRolePermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 21, 2023, 02:51 UTC
- **Edited time:** March 21, 2023, 02:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

Description: Amazon DataZone is a data management service that enables you to catalog, discover, govern, share, and analyze your data. With Amazon DataZone, you can share and access your data across accounts and supported regions. Amazon DataZone simplifies your experience across AWS services, including, but not limited to, Amazon Redshift, Amazon Athena, AWS Glue, and AWS Lake Formation.

AmazonDataZoneRedshiftGlueProvisioningPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneRedshiftGlueProvisioningPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 22, 2023, 20:19 UTC
- **Edited time:** March 12, 2024, 16:44 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

Description: This policy gives Amazon DataZone permissions to publish Amazon Redshift data to the catalog. It also gives Amazon DataZone permissions to grant access or revoke access to Amazon Redshift or Amazon Redshift Serverless published assets in the catalog.

AmazonDataZoneRedshiftManageAccessRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneRedshiftManageAccessRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 22, 2023, 20:15 UTC
- **Edited time:** November 16, 2023, 22:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Description: The AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary policy is the list of permissions that are permitted on an execution role created in a SageMaker environment provisioned by Amazon DataZone.

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 23, 2024, 23:01 UTC
- **Edited time:** May 08, 2024, 02:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
      "servicelog:ProvisionProduct"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
      "servicelog:TerminateProvisionedProduct",
      "servicelog:UpdateProvisionedProduct"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "servicelog: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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

Description: The AmazonDataZoneSageMakerManageAccessRolePolicy policy grants Amazon DataZone the permissions required to grant user access to various resources in the SageMaker environment.

AmazonDataZoneSageMakerManageAccessRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonDataZoneSageMakerManageAccessRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 23, 2024, 23:34 UTC
- **Edited time:** April 23, 2024, 23:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

Description: The AmazonDataZoneSageMakerProvisioningRolePolicy policy grants Amazon DataZone the permissions required to interoperate with Amazon SageMaker.

AmazonDataZoneSageMakerProvisioningRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach `AmazonDataZoneSageMakerProvisioningRolePolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 23, 2024, 23:32 UTC
- **Edited time:** April 23, 2024, 23:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDetectiveFullAccess

Description: Provides full access to Amazon Detective service and scoped access to the console UI dependencies

AmazonDetectiveFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDetectiveFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 30, 2020, 17:57 UTC
- **Edited time:** May 17, 2023, 19:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDetectiveInvestigatorAccess

Description: Provides investigator access to Amazon Detective service and scoped access to the console UI dependencies. This policy grants permission to dive into Detective for investigation purposes and limited write access to Guardduty.

AmazonDetectiveInvestigatorAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDetectiveInvestigatorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 17, 2023, 15:24 UTC
- **Edited time:** November 27, 2023, 03:13 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDetectiveMemberAccess

Description: Provides member access to Amazon Detective service and scoped access to the console UI dependencies.

AmazonDetectiveMemberAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDetectiveMemberAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 17, 2023, 15:16 UTC
- **Edited time:** January 17, 2023, 15:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDetectiveOrganizationsAccess

Description: Provides Organizations access to manage Delegated administrator for Amazon Detective and scoped access to the console UI dependencies. This also grants permission to create a service-linked role for Detective.

AmazonDetectiveOrganizationsAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDetectiveOrganizationsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 02, 2023, 15:20 UTC
- **Edited time:** March 02, 2023, 15:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "detective.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "detective.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
```

```
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : [
      "detective.amazonaws.com",
      "guardduty.amazonaws.com",
      "macie.amazonaws.com",
      "securityhub.amazonaws.com"
    ]
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDetectiveServiceLinkedRolePolicy

Description: Allows Amazon Detective to make service calls on your behalf

AmazonDetectiveServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 18, 2021, 19:47 UTC
- **Edited time:** November 18, 2021, 19:47 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDevOpsGuruConsoleFullAccess

Description: The policy grants full-access to the DevOps Guru console.

AmazonDevOpsGuruConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDevOpsGuruConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 17, 2021, 18:43 UTC
- **Edited time:** August 25, 2022, 18:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDevOpsGuruFullAccess

Description: Provides full access to Amazon DevOps Guru.

AmazonDevOpsGuruFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDevOpsGuruFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 16:38 UTC
- **Edited time:** August 25, 2022, 18:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDevOpsGuruOrganizationsAccess

Description: Provide access to enable and manage Amazon DevOps Guru within an organization.

AmazonDevOpsGuruOrganizationsAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDevOpsGuruOrganizationsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 15, 2021, 23:50 UTC
- **Edited time:** November 15, 2021, 23:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ]
    }
  ]
}
```



```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "OrganizationsDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListAccounts",
      "organizations:ListChildren",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListRoots"
    ],
    "Resource" : "arn:aws:organizations::*"
  },
  {
    "Sid" : "OrganizationsAdminDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DeregisterDelegatedAdministrator",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "devops-guru.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDevOpsGuruReadOnlyAccess

Description: Provides read only access to Amazon DevOps Guru Console.

AmazonDevOpsGuruReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDevOpsGuruReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 16:34 UTC
- **Edited time:** August 25, 2022, 18:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDevOpsGuruServiceRolePolicy

Description: A service-linked role required for Amazon DevOpsGuru to access your resources.

AmazonDevOpsGuruServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 01, 2020, 10:24 UTC
- **Edited time:** January 10, 2023, 14:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDMSCloudWatchLogsRole

Description: Provides access to upload DMS replication logs to cloudwatch logs in customer account.

AmazonDMSCloudWatchLogsRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonDMSCloudWatchLogsRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 07, 2016, 23:44 UTC
- **Edited time:** May 23, 2023, 21:32 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDMSRedshiftS3Role

Description: Provides access to manage S3 settings for Redshift endpoints for DMS.

AmazonDMSRedshiftS3Role is an [AWS managed policy](#).

Using this policy

You can attach AmazonDMSRedshiftS3Role to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2016, 17:05 UTC
- **Edited time:** July 08, 2019, 18:19 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDMSVPCManagementRole

Description: Provides access to manage VPC settings for AWS managed customer configurations

AmazonDMSVPCManagementRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonDMSVPCManagementRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 18, 2015, 16:33 UTC

- **Edited time:** May 23, 2016, 16:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDB-ElasticServiceRolePolicy

Description: Allows Amazon DocumentDB-Elastic to manage AWS resources on your behalf.

AmazonDocDB-ElasticServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 30, 2022, 14:17 UTC
- **Edited time:** November 30, 2022, 14:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
        ]
    }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDBConsoleFullAccess

Description: Provides full access to manage Amazon DocumentDB with MongoDB compatibility using the AWS Management Console. Note this policy also grants full access to publish on all SNS topics within the account, permissions to create and edit Amazon EC2 instances and VPC configurations, permissions to view and list keys on Amazon KMS, and full access to Amazon RDS and Amazon Neptune.

AmazonDocDBConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDocDBConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 09, 2019, 20:37 UTC
- **Edited time:** November 30, 2022, 15:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic>DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic>DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds>DeleteDBCluster",
        "rds>DeleteDBClusterParameterGroup",
        "rds>DeleteDBClusterSnapshot",
```

```
"rds:DeleteDBInstance",
"rds:DeleteDBParameterGroup",
"rds:DeleteDBSubnetGroup",
"rds:DeleteEventSubscription",
"rds:DeleteGlobalCluster",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:ModifyGlobalCluster",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveFromGlobalCluster",
"rds:RemoveRoleFromDBCluster",
```

```
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:AllocateAddress",
    "ec2:AssignIpv6Addresses",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:AssociateRouteTable",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AssociateVpcCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:CreateCustomerGateway",
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc",
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSubnet",
    "ec2:CreateVpc",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
```

```

    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ModifyVpcEndpoint",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "rds.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",

```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDBElasticFullAccess

Description: Provides full access to Amazon DocumentDB Elastic Clusters and other required permissions for its dependencies including EC2, KMS, SecretsManager, CloudWatch and IAM.

AmazonDocDBElasticFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDocDBElasticFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 05, 2023, 13:51 UTC
- **Edited time:** June 21, 2023, 18:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
}

```



```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDBElasticReadOnlyAccess

Description: Provides read-only access to Amazon DocDB-Elastic and CloudWatch metrics.

AmazonDocDBElasticReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDocDBElasticReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 08, 2023, 14:37 UTC
- **Edited time:** June 21, 2023, 16:57 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDBFullAccess

Description: Provides full access to Amazon DocumentDB with MongoDB compatibility. Note this policy also grants full access to publish on all SNS topics within the account and full access to Amazon RDS and Amazon Neptune.

AmazonDocDBFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDocDBFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 09, 2019, 20:21 UTC
- **Edited time:** January 09, 2019, 20:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
```

```
"rds:CopyDBParameterGroup",
"rds:CreateDBCluster",
"rds:CreateDBClusterParameterGroup",
"rds:CreateDBClusterSnapshot",
"rds:CreateDBInstance",
"rds:CreateDBParameterGroup",
"rds:CreateDBSubnetGroup",
"rds:CreateEventSubscription",
"rds>DeleteDBCluster",
"rds>DeleteDBClusterParameterGroup",
"rds>DeleteDBClusterSnapshot",
"rds>DeleteDBInstance",
"rds>DeleteDBParameterGroup",
"rds>DeleteDBSubnetGroup",
"rds>DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
```

```
    "rds:ModifyDBInstance",
    "rds:ModifyDBParameterGroup",
    "rds:ModifyDBSubnetGroup",
    "rds:ModifyEventSubscription",
    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
```

```
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "rds.amazonaws.com"
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDocDBReadOnlyAccess

Description: Provides read-only access to Amazon DocumentDB with MongoDB compatibility. Note that this policy also grants access to Amazon RDS and Amazon Neptune resources.

AmazonDocDBReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDocDBReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 09, 2019, 20:30 UTC
- **Edited time:** January 09, 2019, 20:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDRSVPCManagement

Description: Provides access to manage VPC settings for Amazon managed customer configurations

AmazonDRSVPCManagement is an [AWS managed policy](#).

Using this policy

You can attach AmazonDRSVPCManagement to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 02, 2015, 00:09 UTC
- **Edited time:** September 02, 2015, 00:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDynamoDBFullAccess

Description: Provides full access to Amazon DynamoDB via the AWS Management Console.

AmazonDynamoDBFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDynamoDBFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** January 29, 2021, 17:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

Policy version

Policy version: v15 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDynamoDBFullAccesswithDataPipeline

Description: This policy is on a deprecation path. See documentation for guidance: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>. Provides full access to Amazon DynamoDB including Export/Import using AWS Data Pipeline via the AWS Management Console.

AmazonDynamoDBFullAccesswithDataPipeline is an [AWS managed policy](#).

Using this policy

You can attach AmazonDynamoDBFullAccesswithDataPipeline to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 12, 2015, 02:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```



```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonDynamoDBReadOnlyAccess

Description: Provides read only access to Amazon DynamoDB via the AWS Management Console.

AmazonDynamoDBReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonDynamoDBReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** March 20, 2024, 15:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEBSCSIDriverPolicy

Description: IAM Policy that allows the CSI driver service account to make calls to related services such as EC2 on your behalf.

AmazonEBSCSIDriverPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEBSCSIDriverPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 04, 2022, 17:24 UTC
- **Edited time:** November 18, 2022, 14:42 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerRegistryFullAccess

Description: Provides administrative access to Amazon ECR resources

AmazonEC2ContainerRegistryFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerRegistryFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 21, 2015, 17:06 UTC
- **Edited time:** December 05, 2020, 00:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerRegistryPowerUser

Description: Provides full access to Amazon EC2 Container Registry repositories, but does not allow repository deletion or policy changes.

AmazonEC2ContainerRegistryPowerUser is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerRegistryPowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 21, 2015, 17:05 UTC
- **Edited time:** December 10, 2019, 20:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerRegistryReadOnly

Description: Provides read-only access to Amazon EC2 Container Registry repositories.

AmazonEC2ContainerRegistryReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerRegistryReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 21, 2015, 17:04 UTC
- **Edited time:** December 10, 2019, 20:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerServiceAutoscaleRole

Description: Policy to enable Task Autoscaling for Amazon EC2 Container Service

AmazonEC2ContainerServiceAutoscaleRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerServiceAutoscaleRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 12, 2016, 23:25 UTC
- **Edited time:** February 05, 2018, 19:15 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerServiceEventsRole

Description: Policy to enable CloudWatch Events for EC2 Container Service

AmazonEC2ContainerServiceEventsRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerServiceEventsRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 30, 2017, 16:51 UTC
- **Edited time:** March 06, 2023, 22:25 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerServiceforEC2Role

Description: Default policy for the Amazon EC2 Role for Amazon EC2 Container Service.

AmazonEC2ContainerServiceforEC2Role is an [AWS managed policy](#).

Using this policy

You can attach `AmazonEC2ContainerServiceforEC2Role` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 19, 2015, 18:45 UTC
- **Edited time:** March 06, 2023, 22:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ContainerServiceRole

Description: Default policy for Amazon ECS service role.

AmazonEC2ContainerServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ContainerServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 09, 2015, 16:14 UTC
- **Edited time:** August 11, 2016, 13:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2FullAccess

Description: Provides full access to Amazon EC2 via the AWS Management Console.

AmazonEC2FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 27, 2018, 02:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2ReadOnlyAccess

Description: Provides read only access to Amazon EC2 via the AWS Management Console.

AmazonEC2ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 14, 2024, 18:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2RoleforAWSCodeDeploy

Description: Provides EC2 access to S3 bucket to download revision. This role is needed by the CodeDeploy agent on EC2 instances.

AmazonEC2RoleforAWSCodeDeploy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2RoleforAWSCodeDeploy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 19, 2015, 18:10 UTC

- **Edited time:** March 20, 2017, 17:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2RoleforAWSCodeDeployLimited

Description: Provides EC2 limited access to S3 bucket to download revision. This role is needed by the CodeDeploy agent on EC2 instances.

AmazonEC2RoleforAWSCodeDeployLimited is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2RoleforAWSCodeDeployLimited to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 24, 2020, 17:55 UTC
- **Edited time:** January 20, 2022, 21:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2RoleforDataPipelineRole

Description: Default policy for the Amazon EC2 Role for Data Pipeline service role.

AmazonEC2RoleforDataPipelineRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2RoleforDataPipelineRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 22, 2016, 17:24 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2RoleforSSM

Description: This policy will soon be deprecated. Please use AmazonSSMManagedInstanceCore policy to enable AWS Systems Manager service core functionality on EC2 instances. For more information see <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

AmazonEC2RoleforSSM is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2RoleforSSM to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 29, 2015, 17:48 UTC
- **Edited time:** January 24, 2019, 19:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2RolePolicyForLaunchWizard

Description: Managed policy for the Amazon LaunchWizard service role for EC2

AmazonEC2RolePolicyForLaunchWizard is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2RolePolicyForLaunchWizard to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2019, 08:05 UTC
- **Edited time:** May 16, 2022, 21:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2SpotFleetAutoscaleRole

Description: Policy to enable Autoscaling for Amazon EC2 Spot Fleet

AmazonEC2SpotFleetAutoscaleRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2SpotFleetAutoscaleRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 19, 2016, 18:27 UTC
- **Edited time:** February 18, 2019, 19:17 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEC2SpotFleetTaggingRole

Description: Allows EC2 Spot Fleet to request, terminate and tag Spot Instances on your behalf.

AmazonEC2SpotFleetTaggingRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonEC2SpotFleetTaggingRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 29, 2017, 18:19 UTC
- **Edited time:** April 23, 2020, 19:30 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonECS_FullAccess

Description: Provides administrative access to Amazon ECS resources and enables ECS features through access to other AWS service resources, including VPCs, Auto Scaling groups, and CloudFormation stacks.

AmazonECS_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonECS_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 07, 2017, 21:36 UTC
- **Edited time:** January 04, 2023, 16:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Policy version

Policy version: v20 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

Description: Provides administrative access to Private Certificate Authority, AWS Secrets Manager and other AWS services required to manage ECS Service Connect TLS features on your behalf.

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity is an [AWS managed policy](#).

Using this policy

You can attach

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 19, 2024, 20:08 UTC
- **Edited time:** January 19, 2024, 20:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:RequestTag/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"
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonECSInfrastructureRolePolicyForVolumes

Description: Provides access to other AWS service resources required to manage volumes associated with ECS workloads on your behalf.

AmazonECSInfrastructureRolePolicyForVolumes is an [AWS managed policy](#).

Using this policy

You can attach AmazonECSInfrastructureRolePolicyForVolumes to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 10, 2024, 22:56 UTC
- **Edited time:** January 10, 2024, 22:56 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/AmazonEC2Managed" : "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"
    }
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonECSServiceRolePolicy

Description: Policy to enable Amazon ECS to manage your cluster.

AmazonECSServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 14, 2017, 01:18 UTC
- **Edited time:** December 04, 2023, 19:32 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonECSTaskExecutionRolePolicy

Description: Provides access to other AWS service resources that are required to run Amazon ECS tasks

AmazonECSTaskExecutionRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonECSTaskExecutionRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 16, 2017, 18:48 UTC
- **Edited time:** November 16, 2017, 18:48 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEFSCSIDriverPolicy

Description: Provides management access to EFS resources and read access to EC2

AmazonEFSCSIDriverPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEFSCSIDriverPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** July 25, 2023, 20:10 UTC
- **Edited time:** July 25, 2023, 20:10 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKS_CNI_Policy

Description: This policy provides the Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) the permissions it requires to modify the IP address configuration on your EKS worker nodes. This permission set allows the CNI to list, describe, and modify Elastic Network Interfaces on your behalf. More information on the AWS VPC CNI Plugin is available here: <https://github.com/aws/amazon-vpc-cni-k8s>

AmazonEKS_CNI_Policy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKS_CNI_Policy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2018, 21:07 UTC
- **Edited time:** March 04, 2024, 20:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSClusterPolicy

Description: This policy provides Kubernetes the permissions it requires to manage resources on your behalf. Kubernetes requires Ec2:CreateTags permissions to place identifying information on EC2 resources including but not limited to Instances, Security Groups, and Elastic Network Interfaces.

AmazonEKSClusterPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSClusterPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** May 27, 2018, 21:06 UTC
- **Edited time:** February 07, 2023, 17:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSCoordinatorServiceRolePolicy

Description: This policy allows Amazon EKS to manage AWS resources for EKS connector

AmazonEKSCoordinatorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 04, 2021, 20:31 UTC
- **Edited time:** September 04, 2021, 20:31 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSFargatePodExecutionRolePolicy

Description: Provides access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate

AmazonEKSFargatePodExecutionRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSFargatePodExecutionRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 22, 2019, 04:34 UTC
- **Edited time:** November 22, 2019, 04:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Effect" : "Allow",
"Action" : [
  "ecr:GetAuthorizationToken",
  "ecr:BatchCheckLayerAvailability",
  "ecr:GetDownloadUrlForLayer",
  "ecr:BatchGetImage"
],
"Resource" : "*"
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSFargateServiceRolePolicy

Description: This policy grants necessary permissions to Amazon EKS to run fargate tasks

AmazonEKSFargateServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 22, 2019, 04:36 UTC
- **Edited time:** November 22, 2019, 04:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSLocalOutpostClusterPolicy

Description: This policy provides permissions to EKS local cluster's control-plane instances running in your account to manage resources on your behalf.

AmazonEKSLocalOutpostClusterPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSLocalOutpostClusterPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 24, 2022, 21:56 UTC
- **Edited time:** October 17, 2022, 16:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSLocalOutpostServiceRolePolicy

Description: Allows Amazon EKS Local to call AWS services on your behalf.

AmazonEKSLocalOutpostServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 23, 2022, 21:53 UTC
- **Edited time:** October 24, 2022, 16:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSServicePolicy

Description: This policy allows Amazon Elastic Container Service for Kubernetes to create and manage the necessary resources to operate EKS Clusters.

AmazonEKSServicePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSServicePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2018, 21:08 UTC
- **Edited time:** May 27, 2020, 19:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKSServicePolicy

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSServiceRolePolicy

Description: A Service-Linked Role required for Amazon EKS to call AWS services on your behalf.

AmazonEKSServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 21, 2020, 20:10 UTC
- **Edited time:** May 27, 2020, 19:30 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSVPCResourceController

Description: Policy used by VPC Resource Controller to manage ENI and IPs for worker nodes.

AmazonEKSVPCResourceController is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSVPCResourceController to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 12, 2020, 00:55 UTC
- **Edited time:** August 12, 2020, 00:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEKSWorkerNodePolicy

Description: This policy allows Amazon EKS worker nodes to connect to Amazon EKS Clusters.

AmazonEKSWorkerNodePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonEKSWorkerNodePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2018, 21:09 UTC
- **Edited time:** November 27, 2023, 00:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElastiCacheFullAccess

Description: Provides full access to Amazon ElastiCache via the AWS Management Console.

AmazonElastiCacheFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElastiCacheFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 28, 2023, 03:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElastiCacheReadOnlyAccess

Description: Provides read only access to Amazon ElastiCache via the AWS Management Console.

AmazonElastiCacheReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElastiCacheReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticCacheReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticContainerRegistryPublicFullAccess

Description: Provides administrative access to Amazon ECR Public resources

AmazonElasticContainerRegistryPublicFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonElasticContainerRegistryPublicFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 17:25 UTC
- **Edited time:** December 01, 2020, 17:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticContainerRegistryPublicPowerUser

Description: Provides full access to Amazon ECR Public repositories, but does not allow repository deletion or policy changes.

AmazonElasticContainerRegistryPublicPowerUser is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticContainerRegistryPublicPowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 16:16 UTC
- **Edited time:** December 01, 2020, 16:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticContainerRegistryPublicReadOnly

Description: Provides read-only access to Amazon ECR Public repositories.

AmazonElasticContainerRegistryPublicReadOnly is an [AWS managed policy](#).

Using this policy

You can attach `AmazonElasticContainerRegistryPublicReadOnly` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 17:27 UTC
- **Edited time:** December 01, 2020, 17:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemClientFullAccess

Description: Provides root client access to an Amazon EFS file system

AmazonElasticFileSystemClientFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemClientFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 13, 2020, 16:27 UTC
- **Edited time:** January 13, 2020, 16:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemClientReadOnlyAccess

Description: Provides read only client access to an Amazon EFS file system

AmazonElasticFileSystemClientReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemClientReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** January 13, 2020, 16:24 UTC
- **Edited time:** January 13, 2020, 16:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemClientReadWriteAccess

Description: Provides read and write client access to an Amazon EFS file system

AmazonElasticFileSystemClientReadWriteAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemClientReadWriteAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 13, 2020, 16:21 UTC
- **Edited time:** January 13, 2020, 16:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemFullAccess

Description: Provides full access to Amazon EFS via the AWS Management Console.

AmazonElasticFileSystemFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2015, 16:22 UTC
- **Edited time:** November 28, 2023, 16:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemReadOnlyAccess

Description: Provides read only access to Amazon EFS via the AWS Management Console.

AmazonElasticFileSystemReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2015, 16:25 UTC
- **Edited time:** January 10, 2022, 18:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemServiceRolePolicy

Description: Allows Amazon Elastic File System to manage AWS resources on your behalf

AmazonElasticFileSystemServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 05, 2019, 16:52 UTC
- **Edited time:** January 10, 2022, 19:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticFileSystemsUtils

Description: Allows customers to use AWS Systems Manager to automatically manage Amazon EFS utilities (amazon-efs-utils) package on their EC2 instances, and use CloudWatchLog to get EFS file system mount success/failure notifications.

AmazonElasticFileSystemsUtils is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticFileSystemsUtils to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 29, 2020, 15:16 UTC
- **Edited time:** September 29, 2020, 15:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceEditorsRole

Description: Default policy for the Amazon Elastic MapReduce Editors service role.

AmazonElasticMapReduceEditorsRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceEditorsRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 16, 2018, 21:55 UTC
- **Edited time:** February 09, 2023, 22:39 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceforAutoScalingRole

Description: Amazon Elastic MapReduce for Auto Scaling. Role to allow Auto Scaling to add and remove instances from your EMR cluster.

AmazonElasticMapReduceforAutoScalingRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceforAutoScalingRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 18, 2016, 01:09 UTC
- **Edited time:** November 18, 2016, 01:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
    }
  ],
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceforEC2Role

Description: Default policy for the Amazon Elastic MapReduce for EC2 service role.

AmazonElasticMapReduceforEC2Role is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceforEC2Role to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** August 11, 2017, 23:57 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceFullAccess

Description: This policy is on a deprecation path. See documentation for guidance: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Provides full access to Amazon Elastic MapReduce and underlying services that it requires such as EC2 and S3

AmazonElasticMapReduceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** October 11, 2019, 15:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReducePlacementGroupPolicy

Description: Policy to allow EMR to create, describe and delete EC2 placement groups.

AmazonElasticMapReducePlacementGroupPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReducePlacementGroupPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 29, 2020, 00:37 UTC
- **Edited time:** September 29, 2020, 00:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceReadOnlyAccess

Description: Provides read only access to Amazon Elastic MapReduce via the AWS Management Console.

AmazonElasticMapReduceReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** July 29, 2020, 23:14 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticMapReduceRole

Description: This policy is on a deprecation path. See documentation for guidance: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Default policy for the Amazon Elastic MapReduce service role.

AmazonElasticMapReduceRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticMapReduceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** June 24, 2020, 22:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticsearchServiceRolePolicy

Description: Allow Amazon Elasticsearch Service to access other AWS services such as EC2 Networking APIs on your behalf.

AmazonElasticsearchServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 07, 2017, 00:15 UTC
- **Edited time:** October 23, 2023, 06:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticTranscoder_FullAccess

Description: Grants users full access to Elastic Transcoder and the access to associated services that is required for full Elastic Transcoder functionality.

AmazonElasticTranscoder_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticTranscoder_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 27, 2018, 18:59 UTC

- **Edited time:** June 10, 2019, 22:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticTranscoder_JobsSubmitter

Description: Grants users permission to change presets, submit jobs, and view Elastic Transcoder settings. This policy also grants some read-only access to some other services required to use the Elastic Transcode console, including S3, IAM, and SNS.

AmazonElasticTranscoder_JobsSubmitter is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticTranscoder_JobsSubmitter to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 07, 2018, 21:12 UTC
- **Edited time:** June 10, 2019, 22:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticTranscoder_ReadOnlyAccess

Description: Grants users read-only access to Elastic Transcoder and list access to related services.

AmazonElasticTranscoder_ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticTranscoder_ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 07, 2018, 21:09 UTC
- **Edited time:** June 10, 2019, 22:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonElasticTranscoderRole

Description: Default policy for the Amazon Elastic Transcoder service role.

AmazonElasticTranscoderRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonElasticTranscoderRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** June 13, 2019, 22:48 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRCleanupPolicy

Description: Allows the actions that EMR requires to terminate and delete AWS EC2 resources if the EMR Service role has lost that ability.

AmazonEMRCleanupPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 26, 2017, 23:54 UTC
- **Edited time:** September 29, 2020, 21:11 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
}  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRContainersServiceRolePolicy

Description: Allows access to other AWS service resources that are required to run Amazon EMR

AmazonEMRContainersServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 09, 2020, 00:38 UTC
- **Edited time:** March 10, 2023, 22:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
} ]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRFullAccessPolicy_v2

Description: Provides full access to Amazon EMR

AmazonEMRFullAccessPolicy_v2 is an [AWS managed policy](#).

Using this policy

You can attach AmazonEMRFullAccessPolicy_v2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 12, 2021, 01:50 UTC
- **Edited time:** July 28, 2023, 14:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRReadOnlyAccessPolicy_v2

Description: Provides read only access to Amazon EMR and the associated CloudWatch Metrics.

AmazonEMRReadOnlyAccessPolicy_v2 is an [AWS managed policy](#).

Using this policy

You can attach AmazonEMRReadOnlyAccessPolicy_v2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 12, 2021, 01:39 UTC
- **Edited time:** August 02, 2023, 19:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRServerlessServiceRolePolicy

Description: Allows access to other AWS service resources that are required to run Amazon EMRServerless

AmazonEMRServerlessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 20, 2022, 23:15 UTC
- **Edited time:** January 25, 2024, 18:21 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEMRServicePolicy_v2

Description: This policy is used for the Amazon EMR Service Role and should NOT be used for any other IAM users or roles in your account. The policy grants permissions to create and manage resources associated with EMR and related services necessary for the operation of your EMR cluster.

AmazonEMRServicePolicy_v2 is an [AWS managed policy](#).

Using this policy

You can attach AmazonEMRServicePolicy_v2 to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 12, 2021, 01:11 UTC
- **Edited time:** May 02, 2024, 18:43 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonESCognitoAccess

Description: Provides limited access to the Amazon Cognito configuration service.

AmazonESCognitoAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonESCognitoAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 28, 2018, 22:29 UTC

- **Edited time:** December 20, 2021, 14:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonESFullAccess

Description: Provides full access to the Amazon ES configuration service.

AmazonESFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonESFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 01, 2015, 19:14 UTC
- **Edited time:** October 01, 2015, 19:14 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonESFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonESReadOnlyAccess

Description: Provides read-only access to the Amazon ES configuration service.

AmazonESReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonESReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** October 01, 2015, 19:18 UTC
- **Edited time:** October 03, 2018, 03:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

Description: Allows EventBridge to access Secret Manager resources on your behalf.

AmazonEventBridgeApiDestinationsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 11, 2021, 20:52 UTC
- **Edited time:** February 11, 2021, 20:52 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeFullAccess

Description: Provides full access to Amazon EventBridge.

AmazonEventBridgeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 11, 2019, 14:08 UTC
- **Edited time:** December 01, 2022, 17:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgePipesFullAccess

Description: Provides full access to Amazon EventBridge Pipes.

AmazonEventBridgePipesFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgePipesFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2022, 17:03 UTC
- **Edited time:** December 01, 2022, 17:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgePipesOperatorAccess

Description: Provides read-only and operator (ability to Stop and Start running Pipes) access to Amazon EventBridge Pipes.

AmazonEventBridgePipesOperatorAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgePipesOperatorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2022, 17:04 UTC
- **Edited time:** December 01, 2022, 17:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgePipesReadOnlyAccess

Description: Provides read-only access to Amazon EventBridge Pipes.

AmazonEventBridgePipesReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgePipesReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2022, 17:04 UTC
- **Edited time:** December 01, 2022, 17:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeReadOnlyAccess

Description: Provides read only access to Amazon EventBridge.

AmazonEventBridgeReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 11, 2019, 13:59 UTC
- **Edited time:** December 01, 2022, 17:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeSchedulerFullAccess

Description: The AmazonEventBridgeSchedulerFullAccess managed policy grants permissions to use all EventBridge Scheduler actions for schedules, and schedule groups.

AmazonEventBridgeSchedulerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeSchedulerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 10, 2022, 18:37 UTC
- **Edited time:** November 10, 2022, 18:37 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeSchedulerReadOnlyAccess

Description: The AmazonEventBridgeSchedulerReadOnlyAccess managed policy grants read-only permissions to view details about your schedules and schedule groups

AmazonEventBridgeSchedulerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeSchedulerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 10, 2022, 18:50 UTC
- **Edited time:** November 10, 2022, 18:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
```

```
        "scheduler:ListTagsForResource"  
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeSchemasFullAccess

Description: Provides full access to Amazon EventBridge Schemas.

AmazonEventBridgeSchemasFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeSchemasFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2019, 23:12 UTC
- **Edited time:** November 28, 2019, 23:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeSchemasReadOnlyAccess

Description: Provides read only access to Amazon EventBridge Schemas.

AmazonEventBridgeSchemasReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonEventBridgeSchemasReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2019, 23:05 UTC
- **Edited time:** May 01, 2020, 00:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonEventBridgeSchemasServiceRolePolicy

Description: Grants permissions to Managed Rules created by Amazon EventBridge schemas.

AmazonEventBridgeSchemasServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 27, 2019, 01:10 UTC

- **Edited time:** November 27, 2019, 01:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFISServiceRolePolicy

Description: Policy to enable AWS FIS to manage monitoring and resource selection for experiments.

AmazonFISServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 21, 2020, 21:18 UTC
- **Edited time:** October 25, 2022, 09:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonForecastFullAccess

Description: Gives access to all actions for Amazon Forecast

AmazonForecastFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonForecastFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 18, 2019, 01:52 UTC
- **Edited time:** January 18, 2019, 01:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonForecastFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFraudDetectorFullAccessPolicy

Description: Gives access to all actions for Amazon Fraud Detector

AmazonFraudDetectorFullAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonFraudDetectorFullAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 22:46 UTC
- **Edited time:** December 03, 2019, 22:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFreeRTOSFullAccess

Description: Full Access Policy for Amazon FreeRTOS

AmazonFreeRTOSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonFreeRTOSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 15:32 UTC
- **Edited time:** November 29, 2017, 15:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFreeRTOSOTAUpdate

Description: Allows user to access Amazon FreeRTOS OTA Update

AmazonFreeRTOSOTAUpdate is an [AWS managed policy](#).

Using this policy

You can attach AmazonFreeRTOSOTAUpdate to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 27, 2018, 22:43 UTC
- **Edited time:** December 18, 2020, 17:47 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFSxConsoleFullAccess

Description: Provides full access to Amazon FSx and access to related AWS services via the AWS Management Console.

AmazonFSxConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonFSxConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 16:36 UTC
- **Edited time:** January 10, 2024, 20:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFSxConsoleReadOnlyAccess

Description: Provides read only access to Amazon FSx and access to related AWS services via the AWS Management Console.

AmazonFSxConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonFSxConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** November 28, 2018, 16:35 UTC
- **Edited time:** January 10, 2024, 20:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFSxFullAccess

Description: Provides full access to Amazon FSx and access to related AWS services.

AmazonFSxFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonFSxFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 16:34 UTC
- **Edited time:** January 10, 2024, 20:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Sid" : "ViewAWSDSDirectories",
"Effect" : "Allow",
"Action" : [
  "ds:DescribeDirectories"
],
"Resource" : "*"
},
{
  "Sid" : "FullAccessToFSx",
  "Effect" : "Allow",
  "Action" : [
    "fsx:AssociateFileGateway",
    "fsx:AssociateFileSystemAliases",
    "fsx:CancelDataRepositoryTask",
    "fsx:CopyBackup",
    "fsx:CopySnapshotAndUpdateVolume",
    "fsx>CreateBackup",
    "fsx:CreateDataRepositoryAssociation",
    "fsx:CreateDataRepositoryTask",
    "fsx:CreateFileCache",
    "fsx:CreateFileSystem",
    "fsx:CreateFileSystemFromBackup",
    "fsx:CreateSnapshot",
    "fsx:CreateStorageVirtualMachine",
    "fsx:CreateVolume",
    "fsx:CreateVolumeFromBackup",
    "fsx>DeleteBackup",
    "fsx>DeleteDataRepositoryAssociation",
    "fsx>DeleteFileCache",
    "fsx>DeleteFileSystem",
    "fsx>DeleteSnapshot",
    "fsx>DeleteStorageVirtualMachine",
    "fsx>DeleteVolume",
    "fsx:DescribeAssociatedFileGateways",
    "fsx:DescribeBackups",
    "fsx:DescribeDataRepositoryAssociations",
    "fsx:DescribeDataRepositoryTasks",
    "fsx:DescribeFileCaches",
    "fsx:DescribeFileSystemAliases",
    "fsx:DescribeFileSystems",
    "fsx:DescribeSharedVpcConfiguration",
    "fsx:DescribeSnapshots",
    "fsx:DescribeStorageVirtualMachines",
    "fsx:DescribeVolumes",
```

```

    "fsx:DisassociateFileGateway",
    "fsx:DisassociateFileSystemAliases",
    "fsx:ListTagsForResource",
    "fsx:ManageBackupPrincipalAssociations",
    "fsx:ReleaseFileSystemNfsV3Locks",
    "fsx:RestoreVolumeFromSnapshot",
    "fsx:TagResource",
    "fsx:UntagResource",
    "fsx:UpdateDataRepositoryAssociation",
    "fsx:UpdateFileCache",
    "fsx:UpdateFileSystem",
    "fsx:UpdateSharedVpcConfiguration",
    "fsx:UpdateSnapshot",
    "fsx:UpdateStorageVirtualMachine",
    "fsx:UpdateVolume"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateSLRForFSx",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CreateSLRForLustreS3Integration",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "s3.data-source.lustre.fsx.amazonaws.com"
      ]
    }
  }
},
},

```

```
{
  "Sid" : "CreateLogsForFSxWindowsAuditLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/fsx/*"
  ]
},
{
  "Sid" : "WriteToAmazonKinesisDataFirehose",
  "Effect" : "Allow",
  "Action" : [
    "firehose:PutRecord"
  ],
  "Resource" : [
    "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
  ]
},
{
  "Sid" : "CreateTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DescribeEC2VpcResources",
```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSecurityGroups",
      "ec2:GetSecurityGroupsForVpc",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeRouteTables"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "fsx.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ManageCrossAccountDataReplication",
    "Effect" : "Allow",
    "Action" : [
      "fsx:PutResourcePolicy",
      "fsx:GetResourcePolicy",
      "fsx>DeleteResourcePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "ram.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFSxReadOnlyAccess

Description: Provides read only access to Amazon FSx.

AmazonFSxReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonFSxReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 16:33 UTC
- **Edited time:** November 28, 2018, 16:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonFSxServiceRolePolicy

Description: Allows Amazon FSx to manage AWS resources on your behalf

AmazonFSxServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 28, 2018, 10:38 UTC
- **Edited time:** January 10, 2024, 20:53 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGlacierFullAccess

Description: Provides full access to Amazon Glacier via the AWS Management Console.

AmazonGlacierFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonGlacierFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGlacierReadOnlyAccess

Description: Provides read only access to Amazon Glacier via the AWS Management Console.

AmazonGlacierReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGlacierReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** May 05, 2016, 18:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGrafanaAthenaAccess

Description: This policy grants access to Amazon Athena and the dependencies needed to enable querying and writing results to s3 from the Amazon Athena plugin in Amazon Grafana.

AmazonGrafanaAthenaAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGrafanaAthenaAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 22, 2021, 17:11 UTC
- **Edited time:** November 22, 2021, 17:11 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGrafanaCloudWatchAccess

Description: This policy grants access to Amazon CloudWatch and the dependencies needed to use CloudWatch as a datasource within Amazon Managed Grafana.

AmazonGrafanaCloudWatchAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGrafanaCloudWatchAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 24, 2023, 22:41 UTC
- **Edited time:** March 24, 2023, 22:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGrafanaRedshiftAccess

Description: This policy grants scoped access to Amazon Redshift and the dependencies needed to use the Amazon Redshift plugin in Amazon Grafana.

AmazonGrafanaRedshiftAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGrafanaRedshiftAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 26, 2021, 23:15 UTC
- **Edited time:** November 26, 2021, 23:15 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGrafanaServiceLinkedRolePolicy

Description: Provides access to AWS Resources managed or used by Amazon Grafana.

AmazonGrafanaServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 08, 2022, 23:10 UTC
- **Edited time:** November 08, 2022, 23:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGuardDutyFullAccess

Description: Provides full access to use Amazon GuardDuty.

AmazonGuardDutyFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGuardDutyFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2017, 22:31 UTC
- **Edited time:** June 10, 2024, 22:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
    }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Description: GuardDuty malware protection uses the service-linked role (SLR) named `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. This service-linked role allows GuardDuty malware protection to perform agent-less scans to detect malware. It allows

GuardDuty to create snapshots in your account, and share the snapshots with the GuardDuty service account to scan for malware. It evaluates these shared snapshots and includes the retrieved EC2 instance metadata in the GuardDuty Malware Protection findings. The `AWSServiceRoleForAmazonGuardDutyMalwareProtection` service-linked role trusts the `malware-protection.guardduty.amazonaws.com` service to assume the role.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 19, 2022, 19:06 UTC
- **Edited time:** January 25, 2024, 22:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGuardDutyReadOnlyAccess

Description: Provides read only access to Amazon GuardDuty resources

AmazonGuardDutyReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonGuardDutyReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2017, 22:29 UTC
- **Edited time:** November 16, 2023, 23:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonGuardDutyServiceRolePolicy

Description: Enable access to AWS Resources used or managed by Amazon Guard Duty

AmazonGuardDutyServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 28, 2017, 20:12 UTC
- **Edited time:** March 27, 2024, 00:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHealthLakeFullAccess

Description: Provides full access to Amazon HealthLake service.

AmazonHealthLakeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHealthLakeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 17, 2021, 01:07 UTC
- **Edited time:** February 17, 2021, 01:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHealthLakeReadOnlyAccess

Description: Provides read only access to Amazon HealthLake service.

AmazonHealthLakeReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHealthLakeReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 17, 2021, 02:43 UTC
- **Edited time:** February 17, 2021, 02:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeFullAccess

Description: Provides full access to Honeycode via the AWS Management Console and the SDK.

AmazonHoneycodeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHoneycodeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 20:28 UTC

- **Edited time:** June 24, 2020, 20:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeReadOnlyAccess

Description: Provides read only access to Honeycode via the AWS Management Console and the SDK.

AmazonHoneycodeReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHoneycodeReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 20:28 UTC
- **Edited time:** December 01, 2020, 17:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeServiceRolePolicy

Description: A service-linked role required for Amazon Honeycode to access your resources.

AmazonHoneycodeServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 18, 2020, 18:03 UTC
- **Edited time:** November 18, 2020, 18:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeTeamAssociationFullAccess

Description: Provides full access to Honeycode Team Association via the AWS Management Console and the SDK.

AmazonHoneycodeTeamAssociationFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHoneycodeTeamAssociationFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 20:28 UTC
- **Edited time:** June 24, 2020, 20:28 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

Description: Provides read only access to Honeycode Team Association via the AWS Management Console and the SDK.

AmazonHoneycodeTeamAssociationReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonHoneycodeTeamAssociationReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 20:27 UTC
- **Edited time:** June 24, 2020, 20:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeWorkbookFullAccess

Description: Provides full access to Honeycode Workbook via the AWS Management Console and the SDK.

AmazonHoneycodeWorkbookFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHoneycodeWorkbookFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 20:28 UTC
- **Edited time:** December 01, 2020, 17:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonHoneycodeWorkbookReadOnlyAccess

Description: Provides read only access to Honeycode Workbook via the AWS Management Console and the SDK.

AmazonHoneycodeWorkbookReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonHoneycodeWorkbookReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** June 24, 2020, 20:28 UTC
- **Edited time:** December 01, 2020, 17:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspector2AgentlessServiceRolePolicy

Description: Grants Amazon Inspector access to AWS services needed to perform agent-less security assessments

AmazonInspector2AgentlessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 20, 2023, 15:18 UTC
- **Edited time:** November 20, 2023, 15:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspector2FullAccess

Description: Provides full access to Amazon Inspector and access to other related services such as organizations.

AmazonInspector2FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonInspector2FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 19:10 UTC
- **Edited time:** April 25, 2024, 13:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonInspector2FullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspector2ManagedCisPolicy

Description: This is a managed policy that customer should attach to their roles to communicate with inspector service for CIS scans

AmazonInspector2ManagedCisPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonInspector2ManagedCisPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 24, 2024, 16:31 UTC
- **Edited time:** January 24, 2024, 16:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspector2ReadOnlyAccess

Description: Provides read only access to the Amazon inspector2 service and relevant support services

AmazonInspector2ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonInspector2ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 21, 2022, 14:45 UTC
- **Edited time:** September 22, 2023, 20:56 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspector2ServiceRolePolicy

Description: Grants Amazon Inspector access to AWS services needed to perform security assessments

AmazonInspector2ServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 16, 2021, 20:27 UTC
- **Edited time:** January 22, 2024, 14:06 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy

Policy version

Policy version: v12 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspectorFullAccess

Description: Provides full access to Amazon Inspector.

AmazonInspectorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonInspectorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 07, 2015, 17:08 UTC
- **Edited time:** December 21, 2017, 14:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonInspectorFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspectorReadOnlyAccess

Description: Provides read only access to Amazon Inspector.

AmazonInspectorReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonInspectorReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 07, 2015, 17:08 UTC
- **Edited time:** October 01, 2019, 15:17 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonInspectorServiceRolePolicy

Description: Grants Amazon Inspector access to AWS services needed to perform security assessments

AmazonInspectorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 21, 2017, 15:48 UTC
- **Edited time:** September 11, 2020, 17:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKendraFullAccess

Description: Provides full access to Amazon Kendra via the AWS Management Console.

AmazonKendraFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKendraFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 16:15 UTC
- **Edited time:** December 03, 2019, 16:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKendraFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKendraReadOnlyAccess

Description: Provides read only access to Amazon Kendra via the AWS Management Console.

AmazonKendraReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKendraReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** December 03, 2019, 16:13 UTC
- **Edited time:** May 27, 2021, 17:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKeyspacesFullAccess

Description: Provide full access to Amazon Keyspaces

AmazonKeyspacesFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKeyspacesFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 23, 2020, 17:06 UTC
- **Edited time:** October 03, 2023, 19:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKeyspacesReadOnlyAccess

Description: Provide read only access to Amazon Keyspaces

AmazonKeyspacesReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKeyspacesReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** April 23, 2020, 17:07 UTC
- **Edited time:** July 07, 2022, 14:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKeyspacesReadOnlyAccess_v2

Description: Provide read only access to Amazon Keyspaces and related AWS services.

AmazonKeyspacesReadOnlyAccess_v2 is an [AWS managed policy](#).

Using this policy

You can attach AmazonKeyspacesReadOnlyAccess_v2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 12, 2023, 17:01 UTC
- **Edited time:** September 12, 2023, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisAnalyticsFullAccess

Description: Provides full access to Amazon Kinesis Analytics via the AWS Management Console.

AmazonKinesisAnalyticsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisAnalyticsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 21, 2016, 19:01 UTC
- **Edited time:** September 21, 2016, 19:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisAnalyticsReadOnly

Description: Provides read-only access to Amazon Kinesis Analytics via the AWS Management Console.

AmazonKinesisAnalyticsReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisAnalyticsReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 21, 2016, 18:16 UTC
- **Edited time:** September 21, 2016, 18:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisFirehoseFullAccess

Description: Provides full access to all Amazon Kinesis Firehose Delivery Streams.

AmazonKinesisFirehoseFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisFirehoseFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 07, 2015, 18:45 UTC
- **Edited time:** October 07, 2015, 18:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisFirehoseReadOnlyAccess

Description: Provides read only access to all Amazon Kinesis Firehose Delivery Streams.

AmazonKinesisFirehoseReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisFirehoseReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 07, 2015, 18:43 UTC
- **Edited time:** October 07, 2015, 18:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisFullAccess

Description: Provides full access to all streams via the AWS Management Console.

AmazonKinesisFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisReadOnlyAccess

Description: Provides read only access to all streams via the AWS Management Console.

AmazonKinesisReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisVideoStreamsFullAccess

Description: Provides full access to Amazon Kinesis Video Streams via the AWS Management Console.

AmazonKinesisVideoStreamsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisVideoStreamsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2017, 23:27 UTC
- **Edited time:** December 01, 2017, 23:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonKinesisVideoStreamsReadOnlyAccess

Description: Provides read only access to AWS Kinesis Video Streams via the AWS Management Console.

AmazonKinesisVideoStreamsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonKinesisVideoStreamsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2017, 23:14 UTC
- **Edited time:** December 01, 2017, 23:14 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLaunchWizard_Fullaccess

Description: Full access to AWS Launch wizard and other required services.

AmazonLaunchWizard_Fullaccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonLaunchWizard_Fullaccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 06, 2020, 17:47 UTC
- **Edited time:** February 22, 2023, 17:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Policy version

Policy version: v15 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
```

```
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AllocateHosts",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:CreateDhcpOptions",
    "ec2:CreateEgressOnlyInternetGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateVolume",
    "ec2:CreateVpcEndpoint",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVolumeAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:AssociateDhcpOptions",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:AttachVolume",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteKeyPair",
    "ec2>DeleteNatGateway",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteVolume",
    "ec2>DeleteVpc",
    "ec2:DetachInternetGateway",
    "ec2:DetachVolume",
    "ec2>DeleteSnapshot",
    "ec2:AssociateRouteTable",
    "ec2:AssociateVpcCidrBlock",
    "ec2>DeleteNetworkAcl",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2>DeleteSubnet",
    "ec2:DetachNetworkInterface",
```

```

    "ec2:DisassociateAddress",
    "ec2:DisassociateVpcCidrBlock",
    "ec2:GetLaunchTemplateData",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:GetConsoleOutput",
    "ec2:GetPasswordData",
    "ec2:ReleaseAddress",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem:DeleteFileSystem",
    "elasticfilesystem:DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",
    "cloudformation>DeleteStack"
  ]
}

```

```

    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
      "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/**"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
      "arn:aws:iam:*:*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ],
    "Condition" : {

```

```

    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling>CreateOrUpdateTags",
      "logs:CreateLogStream",
      "logs>DeleteLogGroup",
      "logs>DeleteLogStream",
      "logs:DescribeLog*",
      "logs:PutLogEvents",
      "resource-groups:CreateGroup",
      "resource-groups>DeleteGroup",
      "sns:ListSubscriptionsByTopic",
      "sns:Publish",
      "ssm>DeleteDocument",
      "ssm>DeleteParameter*",
      "ssm:DescribeDocument*",
      "ssm:GetDocument",
      "ssm:PutParameter"
    ],
    "Resource" : [
      "arn:aws:resource-groups:*:*:group/LaunchWizard*",
      "arn:aws:sns:*:*:*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
      "arn:aws:ssm:*:*:parameter/LaunchWizard*",
      "arn:aws:ssm:*:*:document/LaunchWizard*",
      "arn:aws:logs:*:*:log-group:*:*:*"
    ]
  }
}

```

```

    "arn:aws:logs:*:*:log-group:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-RunShellScript"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs>DeleteLogStream",
    "logs:GetLogEvents",
    "logs:PutLogEvents",
    "ssm:AddTagsToResource",
    "ssm:DescribeDocument",
    "ssm:GetDocument",
    "ssm:ListTagsForResource",
    "ssm:RemoveTagsFromResource"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*:*:*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*",
    "arn:aws:ssm:*:*:parameter/LaunchWizard*",

```

```
    "arn:aws:ssm:*:*:document/LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*",
    "cloudformation:DescribeAccountLimits",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:List*",
    "cloudformation:ValidateTemplate",
    "ds:Describe*",
    "ds:ListAuthorizedApplications",
    "ec2:Describe*",
    "ec2:Get*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:List*",
    "logs:CreateLogGroup",
    "logs:GetLogDelivery",
    "logs:GetLogRecord",
    "logs:ListLogDeliveries",
    "resource-groups:Get*",
    "resource-groups:List*",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListServiceQuotas",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "ssm:CreateDocument",
    "ssm:DescribeAutomation*",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeParameters",
    "ssm:GetAutomationExecution",
    "ssm:GetCommandInvocation",
    "ssm:GetParameter*",
    "ssm:GetConnectionStatus",
    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution",
      "ssm:StopAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:GetLog*",
    "Resource" : [
      "arn:aws:logs:*:*:log-group:*:*:*",
      "arn:aws:logs:*:*:log-group:LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:List*",
      "cloudformation:Describe*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "application-insights.amazonaws.com",
          "events.amazonaws.com",
```

```
        "autoscaling.amazonaws.com.cn",
        "events.amazonaws.com.cn"
    ]
}
},
{
    "Effect" : "Allow",
    "Action" : "launchwizard:*",
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs>DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs>CreateQueue",
        "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "cloudformation>CreateStack",
        "route53:ListHostedZones",
```



```

    "ec2:CreateSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateFileSystem",
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:s3:::launchwizard*/**",
    "arn:aws:s3:::aws-sap-data-provider/config.properties"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "cloudformation:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3>DeleteBucket",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction"
  ],

```

```
"Resource" : [
  "arn:aws:lambda:*:*:function:LaunchWizard*",
  "arn:aws:s3:::launchwizard*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
```

```
    "Effect" : "Allow",
    "Action" : "ssm:DeleteOpsMetadata",
    "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:DeleteTopic",
      "sns:Subscribe",
      "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:UntagResource",
      "fsx:TagResource",
      "fsx>DeleteFileSystem",
      "fsx:ListTagsForResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/Name" : "LaunchWizard*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateFileSystem"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/Name" : [
          "LaunchWizard*"
        ]
      }
    }
  }
},
{
```

```

    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:CreatePortfolio",
      "servicecatalog:DescribePortfolio",
      "servicecatalog:CreateConstraint",
      "servicecatalog:CreateProduct",
      "servicecatalog:AssociatePrincipalWithPortfolio",
      "servicecatalog:CreateProvisioningArtifact",
      "servicecatalog:TagResource",
      "servicecatalog:UntagResource"
    ],
    "Resource" : [
      "arn:aws:servicecatalog:*:*:*/*",
      "arn:aws:catalog:*:*:*/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "VisualEditor0",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateAssociation",
      "ssm>DeleteAssociation"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",

```

```
"Action" : [
  "elasticfilesystem:UntagResource",
  "elasticfilesystem:TagResource"
],
"Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "launchwizard.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:TagResource",
    "logs:UntagResource"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLaunchWizardFullAccessV2

Description: Full access to AWS Launch wizard and other required services.

AmazonLaunchWizardFullAccessV2 is an [AWS managed policy](#).

Using this policy

You can attach AmazonLaunchWizardFullAccessV2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 01, 2023, 17:14 UTC
- **Edited time:** September 01, 2023, 17:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexChannelsAccess

Description: This policy allows customers to call Lex runtime from channels

AmazonLexChannelsAccess is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 13, 2021, 20:12 UTC
- **Edited time:** January 13, 2021, 20:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Action" : [
      "lex:ListBots"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexFullAccess

Description: Provides full access to Amazon Lex via the AWS Management Console. Also provides access to create Lex Service Linked Roles and grant Lex permissions to invoke a limited set of Lambda functions.

AmazonLexFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLexFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 11, 2017, 23:20 UTC
- **Edited time:** April 16, 2024, 20:06 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLexFullAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexReadOnly

Description: Provides read-only access to Amazon Lex.

AmazonLexReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonLexReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 11, 2017, 23:13 UTC
- **Edited time:** May 13, 2024, 16:58 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLexReadOnly

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexReplicationPolicy

Description: Allows Amazon Lex to replicate Lex resources across regions on your behalf.

AmazonLexReplicationPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 31, 2024, 23:29 UTC
- **Edited time:** March 08, 2024, 17:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexRunBotsOnly

Description: Provides access to Amazon Lex conversational APIs.

AmazonLexRunBotsOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonLexRunBotsOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 11, 2017, 23:06 UTC
- **Edited time:** August 18, 2021, 00:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLexV2BotPolicy

Description: Provides Lex V2 bots access to call other AWS services on your behalf.

AmazonLexV2BotPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 13, 2021, 20:10 UTC
- **Edited time:** January 13, 2021, 20:10 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutEquipmentFullAccess

Description: Provides full access to Amazon Lookout for Equipment operations

AmazonLookoutEquipmentFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutEquipmentFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 08, 2021, 15:52 UTC
- **Edited time:** November 24, 2021, 21:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutEquipmentReadOnlyAccess

Description: Provides read only access to Amazon Lookout for Equipments

AmazonLookoutEquipmentReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutEquipmentReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 05, 2021, 16:47 UTC
- **Edited time:** November 10, 2022, 22:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutMetricsFullAccess

Description: Gives access to all actions for Amazon Lookout for Metrics

AmazonLookoutMetricsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutMetricsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 07, 2021, 00:43 UTC
- **Edited time:** May 07, 2021, 00:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutMetricsReadOnlyAccess

Description: Gives access to all read-only actions for Amazon Lookout for Metrics

AmazonLookoutMetricsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutMetricsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 07, 2021, 00:43 UTC
- **Edited time:** January 04, 2022, 18:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutVisionConsoleFullAccess

Description: Provides full access to Amazon Lookout for Vision and scoped access to required service and console dependencies.

AmazonLookoutVisionConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutVisionConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2021, 19:37 UTC
- **Edited time:** May 11, 2021, 19:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutVisionConsoleReadOnlyAccess

Description: Provides read only access to Amazon Lookout for Vision and scoped access to required service and console dependencies.

AmazonLookoutVisionConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutVisionConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2021, 19:32 UTC
- **Edited time:** December 09, 2021, 02:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutVisionFullAccess

Description: Provides full access to Amazon Lookout for Vision and scoped access to required dependencies.

AmazonLookoutVisionFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutVisionFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2021, 19:24 UTC
- **Edited time:** May 11, 2021, 19:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonLookoutVisionReadOnlyAccess

Description: Provides read only access to Amazon Lookout for Vision and scoped access to required dependencies.

AmazonLookoutVisionReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonLookoutVisionReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2021, 19:11 UTC
- **Edited time:** December 09, 2021, 03:01 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningBatchPredictionsAccess

Description: Grants users permission to request Amazon Machine Learning batch predictions.

AmazonMachineLearningBatchPredictionsAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningBatchPredictionsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 17:12 UTC
- **Edited time:** April 09, 2015, 17:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ]
    }
  ]
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningCreateOnlyAccess

Description: Provides create access for non-prediction Amazon Machine Learning resources.

AmazonMachineLearningCreateOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningCreateOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 17:18 UTC
- **Edited time:** June 29, 2016, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningFullAccess

Description: Provides full access to Amazon Machine Learning resources.

AmazonMachineLearningFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** April 09, 2015, 17:25 UTC
- **Edited time:** April 09, 2015, 17:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Description: Grants users permission to create and delete the real-time endpoint for Amazon Machine Learning models.

AmazonMachineLearningManageRealTimeEndpointOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningManageRealTimeEndpointOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 17:32 UTC
- **Edited time:** April 09, 2015, 17:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningReadOnlyAccess

Description: Provides read only access to Amazon Machine Learning resources.

AmazonMachineLearningReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 17:40 UTC
- **Edited time:** April 09, 2015, 17:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "machinelearning:Describe*",
      "machinelearning:Get*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

Description: Grants users permission to request Amazon Machine Learning real-time predictions.

AmazonMachineLearningRealTimePredictionOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMachineLearningRealTimePredictionOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 17:44 UTC
- **Edited time:** April 09, 2015, 17:44 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

Description: Allows Machine Learning to configure and use your Redshift Clusters and S3 Staging Locations for Redshift Data Source.

AmazonMachineLearningRoleforRedshiftDataSourceV3 is an [AWS managed policy](#).

Using this policy

You can attach `AmazonMachineLearningRoleforRedshiftDataSourceV3` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 24, 2020, 18:00 UTC
- **Edited time:** June 24, 2020, 18:00 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMacieFullAccess

Description: Provides full access to Amazon Macie.

AmazonMacieFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMacieFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 14, 2017, 14:54 UTC

- **Edited time:** July 01, 2022, 00:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMacieFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMacieHandshakeRole

Description: Grants permission to create the service-linked role of Amazon Macie.

AmazonMacieHandshakeRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonMacieHandshakeRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 28, 2018, 15:46 UTC
- **Edited time:** June 28, 2018, 15:46 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AWSServiceName" : "macie.amazonaws.com"
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMacieReadOnlyAccess

Description: Provides readonly access to Amazon Macie.

AmazonMacieReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMacieReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 15, 2023, 21:50 UTC
- **Edited time:** June 15, 2023, 21:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMacieServiceRole

Description: Grants Macie read-only access to resource dependencies in your account in order to enable data analysis.

AmazonMacieServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonMacieServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 14:53 UTC
- **Edited time:** August 14, 2017, 14:53 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMacieServiceRolePolicy

Description: Service linked role for Amazon Macie

AmazonMacieServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 19, 2018, 22:17 UTC
- **Edited time:** May 19, 2022, 19:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
  ]
}

```

```
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonManagedBlockchainConsoleFullAccess

Description: Provides full access to Amazon Managed Blockchain via the AWS Management Console

AmazonManagedBlockchainConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonManagedBlockchainConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 29, 2019, 21:23 UTC
- **Edited time:** April 29, 2019, 21:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "managedblockchain:*",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:CreateVpcEndpoint",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonManagedBlockchainFullAccess

Description: Provides full access to Amazon Managed Blockchain.

AmazonManagedBlockchainFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonManagedBlockchainFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 29, 2019, 21:39 UTC

- **Edited time:** April 29, 2019, 21:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonManagedBlockchainReadOnlyAccess

Description: Provides read-only access to Amazon Managed Blockchain.

AmazonManagedBlockchainReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonManagedBlockchainReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 30, 2019, 18:17 UTC
- **Edited time:** April 30, 2019, 18:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonManagedBlockchainServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Amazon Managed Blockchain

AmazonManagedBlockchainServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 17, 2020, 19:51 UTC
- **Edited time:** January 17, 2020, 19:51 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMCSFullAccess

Description: Provide full access to Amazon Managed Apache Cassandra Service

AmazonMCSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMCSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 13:45 UTC
- **Edited time:** April 17, 2020, 19:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMCSFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMCSReadOnlyAccess

Description: Provide read only access to Amazon Managed Apache Cassandra Service

AmazonMCSReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMCSReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 13:46 UTC
- **Edited time:** April 17, 2020, 19:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMechanicalTurkFullAccess

Description: Provides full access to all APIs in Amazon Mechanical Turk.

AmazonMechanicalTurkFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMechanicalTurkFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 11, 2015, 19:08 UTC
- **Edited time:** December 11, 2015, 19:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMechanicalTurkReadOnly

Description: Provides access to read only APIs in Amazon Mechanical Turk.

AmazonMechanicalTurkReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonMechanicalTurkReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 11, 2015, 19:08 UTC
- **Edited time:** September 25, 2019, 21:06 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMemoryDBFullAccess

Description: Provides full access to Amazon MemoryDB via the AWS Management Console.

AmazonMemoryDBFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMemoryDBFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 08, 2021, 19:24 UTC
- **Edited time:** October 08, 2021, 19:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMemoryDBReadOnlyAccess

Description: Provides read only access to Amazon MemoryDB via the AWS Management Console.

AmazonMemoryDBReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMemoryDBReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 08, 2021, 19:27 UTC
- **Edited time:** October 08, 2021, 19:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMobileAnalyticsFinancialReportAccess

Description: Provides read only access to all reports including financial data for all application resources.

AmazonMobileAnalyticsFinancialReportAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMobileAnalyticsFinancialReportAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMobileAnalyticsFullAccess

Description: Provides full access to all application resources.

AmazonMobileAnalyticsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMobileAnalyticsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMobileAnalyticsNon-financialReportAccess

Description: Provides read only access to non financial reports for all application resources.

AmazonMobileAnalyticsNon-financialReportAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMobileAnalyticsNon-financialReportAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMobileAnalyticsWriteOnlyAccess

Description: Provides write only access to put event data for all application resources. (Recommended for SDK integration)

AmazonMobileAnalyticsWriteOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMobileAnalyticsWriteOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMonitronFullAccess

Description: Provides full access to manage Amazon Monitron

AmazonMonitronFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMonitronFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 02, 2020, 22:40 UTC
- **Edited time:** June 08, 2022, 16:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMonitronFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMQApiFullAccess

Description: Provides full access to AmazonMQ via our API/SDK.

AmazonMQApiFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMQApiFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 18, 2018, 20:31 UTC
- **Edited time:** November 04, 2020, 16:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMQApiFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMQApiReadOnlyAccess

Description: Provides read only access to AmazonMQ via our API/SDK.

AmazonMQApiReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMQApiReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 18, 2018, 20:31 UTC
- **Edited time:** December 18, 2018, 20:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",

```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMQFullAccess

Description: Provides full access to AmazonMQ via the AWS Management Console.

AmazonMQFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMQFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2017, 15:28 UTC
- **Edited time:** November 04, 2020, 16:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMQFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMQReadOnlyAccess

Description: Provides read only access to AmazonMQ via the AWS Management Console.

AmazonMQReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMQReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2017, 15:30 UTC
- **Edited time:** November 28, 2017, 19:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMQServiceRolePolicy

Description: Service Linked Role Policy for AWS Amazon MQ

AmazonMQServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 04, 2020, 16:07 UTC
- **Edited time:** November 04, 2020, 16:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMSKConnectReadOnlyAccess

Description: Provide readonly access to Amazon MSK Connect

AmazonMSKConnectReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMSKConnectReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 20, 2021, 10:18 UTC
- **Edited time:** October 18, 2021, 09:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    ]
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMSKFullAccess

Description: Provide full access to Amazon MSK and other required permissions for its dependencies.

AmazonMSKFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMSKFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 14, 2019, 22:07 UTC
- **Edited time:** October 18, 2023, 11:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonMSKFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMSKReadOnlyAccess

Description: Provide readonly access to Amazon MSK

AmazonMSKReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonMSKReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 14, 2019, 22:28 UTC
- **Edited time:** January 14, 2019, 22:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonMWAAServiceRolePolicy

Description: The Service Linked Role used by Amazon Managed Workflows for Apache Airflow.

AmazonMWAAServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 24, 2020, 14:13 UTC
- **Edited time:** November 17, 2022, 00:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonNimbleStudio-LaunchProfileWorker

Description: This policy grants access to resources needed by Nimble Studio Launch Profile workers. Attach this policy to EC2 instances created by Nimble Studio Builder.

AmazonNimbleStudio-LaunchProfileWorker is an [AWS managed policy](#).

Using this policy

You can attach AmazonNimbleStudio-LaunchProfileWorker to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 28, 2021, 04:47 UTC
- **Edited time:** April 28, 2021, 04:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonNimbleStudio-StudioAdmin

Description: This policy grants access to Amazon Nimble Studio resources associated with the studio admin and related studio resources in other services. Attach this policy to the Admin role associated with your studio.

AmazonNimbleStudio-StudioAdmin is an [AWS managed policy](#).

Using this policy

You can attach AmazonNimbleStudio-StudioAdmin to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 28, 2021, 04:47 UTC
- **Edited time:** September 22, 2023, 17:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonNimbleStudio-StudioUser

Description: This policy grants access to Amazon Nimble Studio resources associated with the studio user and related studio resources in other services. Attach this policy to the User role associated with your studio.

AmazonNimbleStudio-StudioUser is an [AWS managed policy](#).

Using this policy

You can attach AmazonNimbleStudio-StudioUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 28, 2021, 04:48 UTC
- **Edited time:** September 22, 2023, 17:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOmicsFullAccess

Description: Provides full access to Amazon Omics and other required AWS services. This policy allows the user to view and accept RAM share invitations to access resources outside of the user's AWS account.

AmazonOmicsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOmicsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 24, 2023, 00:59 UTC
- **Edited time:** February 24, 2023, 00:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOmicsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOmicsReadOnlyAccess

Description: Provide read only access to Amazon Omics

AmazonOmicsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOmicsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2022, 04:17 UTC
- **Edited time:** November 29, 2022, 04:17 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOneEnterpriseFullAccess

Description: This policy grants administrative permissions that allow access to all Amazon One Enterprise resources and operations.

AmazonOneEnterpriseFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOneEnterpriseFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2023, 04:58 UTC
- **Edited time:** November 28, 2023, 04:58 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOneEnterpriseInstallerAccess

Description: This policy grants limited read and write permissions that allow device installation and activation.

AmazonOneEnterpriseInstallerAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOneEnterpriseInstallerAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2023, 05:00 UTC
- **Edited time:** November 28, 2023, 05:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",

```

```
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOneEnterpriseReadOnlyAccess

Description: This policy grants read only permissions to all Amazon One Enterprise resources and operations.

AmazonOneEnterpriseReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOneEnterpriseReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2023, 04:59 UTC
- **Edited time:** November 28, 2023, 04:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchDashboardsServiceRolePolicy

Description: Provides access to Amazon OpenSearch Dashboards Service to access other AWS services such as CloudWatch on your behalf

AmazonOpenSearchDashboardsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 22, 2023, 19:38 UTC
- **Edited time:** December 22, 2023, 19:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

Description: Allows OpenSearch DirectQuery Service to access AWS Glue APIs for creating resources on your behalf.

AmazonOpenSearchDirectQueryGlueCreateAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchDirectQueryGlueCreateAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 06, 2024, 12:24 UTC
- **Edited time:** May 06, 2024, 12:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchIngestionFullAccess

Description: Allows Amazon OpenSearch Ingestion to access other AWS services on your behalf.

AmazonOpenSearchIngestionFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchIngestionFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 26, 2023, 18:11 UTC
- **Edited time:** April 26, 2023, 18:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchIngestionReadOnlyAccess

Description: Provides read only access to the Amazon OpenSearch Ingestion Service

AmazonOpenSearchIngestionReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchIngestionReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 26, 2023, 18:09 UTC
- **Edited time:** April 26, 2023, 18:09 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "osis:GetPipeline",
      "osis:GetPipelineChangeProgress",
      "osis:GetPipelineBlueprint",
      "osis:ListPipelineBlueprints",
      "osis:ListPipelines",
      "osis:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchIngestionServiceRolePolicy

Description: Allows Amazon OpenSearch Ingestion Service to access other AWS services on your behalf.

AmazonOpenSearchIngestionServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 18, 2022, 16:49 UTC

- **Edited time:** November 18, 2022, 16:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchServerlessServiceRolePolicy

Description: Allow Amazon OpenSearch Serverless to access other AWS services such as CloudWatch APIs on your behalf.

AmazonOpenSearchServerlessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 24, 2022, 19:50 UTC
- **Edited time:** November 24, 2022, 19:50 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchServiceCognitoAccess

Description: Provides access to the Amazon Cognito configuration service.

AmazonOpenSearchServiceCognitoAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchServiceCognitoAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 02, 2021, 06:31 UTC
- **Edited time:** December 20, 2021, 14:04 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchServiceFullAccess

Description: Provides full access to the Amazon OpenSearch Service configuration service.

AmazonOpenSearchServiceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchServiceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 08, 2021, 05:33 UTC
- **Edited time:** September 08, 2021, 05:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchServiceReadOnlyAccess

Description: Provides read-only access to the Amazon OpenSearch Service configuration service.

AmazonOpenSearchServiceReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonOpenSearchServiceReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 08, 2021, 05:38 UTC
- **Edited time:** September 08, 2021, 05:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonOpenSearchServiceRolePolicy

Description: Allow Amazon OpenSearch Service to access other AWS services such as EC2 Networking APIs on your behalf.

AmazonOpenSearchServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 26, 2021, 09:27 UTC
- **Edited time:** October 23, 2023, 07:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*:*:vpn/*",
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPersonalizeFullAccess

Description: Provides full access to Amazon Personalize via the AWS Management Console and SDK. Also provides select access to related services (e.g., S3, CloudWatch).

AmazonPersonalizeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPersonalizeFullAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 04, 2018, 22:24 UTC
- **Edited time:** May 30, 2019, 23:46 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPollyFullAccess

Description: Grants full access to Amazon Polly service and resources.

AmazonPollyFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPollyFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2016, 18:59 UTC
- **Edited time:** November 30, 2016, 18:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonPollyFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPollyReadOnlyAccess

Description: Grants read-only access to Amazon Polly resources.

AmazonPollyReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPollyReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2016, 18:59 UTC
- **Edited time:** July 17, 2018, 16:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPrometheusConsoleFullAccess

Description: Grants full access to AWS Managed Prometheus resources in the AWS console

AmazonPrometheusConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPrometheusConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 18:11 UTC
- **Edited time:** October 24, 2022, 22:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPrometheusFullAccess

Description: Grants full access to AWS Managed Prometheus resources

AmazonPrometheusFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPrometheusFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 18:10 UTC
- **Edited time:** November 26, 2023, 20:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPrometheusQueryAccess

Description: Grants access to run queries against AWS Managed Prometheus resources

AmazonPrometheusQueryAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPrometheusQueryAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 19, 2020, 01:02 UTC
- **Edited time:** December 19, 2020, 01:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPrometheusRemoteWriteAccess

Description: Grants write only access to AWS Managed Prometheus workspaces

AmazonPrometheusRemoteWriteAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonPrometheusRemoteWriteAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 19, 2020, 01:04 UTC
- **Edited time:** December 19, 2020, 01:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Action" : [
      "aps:RemoteWrite"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonPrometheusScrapperServiceRolePolicy

Description: Provides access to AWS Resources managed or used by Amazon Managed Service for Prometheus Collector

AmazonPrometheusScrapperServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2023, 14:19 UTC
- **Edited time:** April 26, 2024, 20:25 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScrapper"
          ]
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid" : "TagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "Null" : {
        "aws:RequestTag/AMPAgentlessScrapper" : "false"
      }
    }
  },
  {
    "Sid" : "ENIUpdating",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AMPAgentlessScrapper" : "false"
      }
    }
  },
  {
    "Sid" : "EKSAccess",
    "Effect" : "Allow",
    "Action" : "eks:DescribeCluster",
    "Resource" : "arn:aws:eks:*:*:cluster/*"
  },
  {
    "Sid" : "DeleteEKSAccessEntry",
    "Effect" : "Allow",
    "Action" : "eks:DeleteAccessEntry",
    "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
}
```

```
    },
    "ArnLike" : {
      "eks:principalArn" : "arn:aws:iam:*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
    }
  },
  {
    "Sid" : "APSWriting",
    "Effect" : "Allow",
    "Action" : "aps:RemoteWrite",
    "Resource" : "arn:aws:aps:*:*:workspace/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonQFullAccess

Description: Provides full access to enable interactions with Amazon Q

AmazonQFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonQFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2023, 16:00 UTC

- **Edited time:** April 29, 2024, 17:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonQFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonQLDBConsoleFullAccess

Description: Provides full access to Amazon QLDB via the AWS Management Console.

AmazonQLDBConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonQLDBConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 05, 2019, 18:24 UTC
- **Edited time:** November 04, 2022, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonQLDBFullAccess

Description: Provides full access to Amazon QLDB via the service API.

AmazonQLDBFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonQLDBFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 05, 2019, 18:23 UTC

- **Edited time:** November 04, 2022, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonQLDBFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonQLDBReadOnly

Description: Provides read only access to Amazon QLDB.

AmazonQLDBReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonQLDBReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 05, 2019, 18:19 UTC
- **Edited time:** July 02, 2021, 02:17 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonQLDBReadOnly

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSBetaServiceRolePolicy

Description: Allows Amazon RDS to manage AWS resources on your behalf.

AmazonRDSBetaServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 02, 2018, 19:41 UTC
- **Edited time:** December 14, 2022, 18:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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"
      }
    }
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSCustomInstanceProfileRolePolicy

Description: Allows Amazon RDS Custom to perform various automation actions and database management tasks through an EC2 instance profile.

AmazonRDSCustomInstanceProfileRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSCustomInstanceProfileRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 27, 2024, 17:42 UTC
- **Edited time:** February 27, 2024, 17:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSCustomPreviewServiceRolePolicy

Description: Amazon RDS Custom Preview Service Role Policy

AmazonRDSCustomPreviewServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 08, 2021, 21:44 UTC
- **Edited time:** September 20, 2023, 17:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSCustomServiceRolePolicy

Description: Allows Amazon RDS Custom to manage AWS resources on your behalf.

AmazonRDSCustomServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 08, 2021, 21:39 UTC

- **Edited time:** April 19, 2024, 15:15 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSDDataFullAccess

Description: Allows full access to use the RDS data APIs, secret store APIs for RDS database credentials, and DB console query management APIs to execute SQL statements on Aurora Serverless clusters in the AWS account.

AmazonRDSDDataFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSDDataFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 20, 2018, 21:29 UTC
- **Edited time:** November 20, 2019, 21:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSDirectoryServiceAccess

Description: Allow RDS to access Directory Service Managed AD on behalf of the customer for domain-joined SQL Server DB instances.

AmazonRDSDirectoryServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSDirectoryServiceAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 26, 2016, 02:02 UTC
- **Edited time:** May 15, 2019, 16:51 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSEnhancedMonitoringRole

Description: Provides access to Cloudwatch for RDS Enhanced Monitoring

AmazonRDSEnhancedMonitoringRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSEnhancedMonitoringRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 11, 2015, 19:58 UTC
- **Edited time:** November 11, 2015, 19:58 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSFullAccess

Description: Provides full access to Amazon RDS via the AWS Management Console.

AmazonRDSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** August 17, 2023, 23:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRDSFullAccess

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSPerformanceInsightsFullAccess

Description: Provides full access to RDS Performance Insights via the AWS Management Console

AmazonRDSPerformanceInsightsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSPerformanceInsightsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 15, 2023, 23:41 UTC
- **Edited time:** October 23, 2023, 21:14 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSPerformanceInsightsReadOnly

Description: Read-Only policy for RDS Performance Insights

AmazonRDSPerformanceInsightsReadOnly is an [AWS managed policy](#).

Using this policy

You can attach `AmazonRDSPerformanceInsightsReadOnly` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 05, 2022, 00:02 UTC
- **Edited time:** October 23, 2023, 21:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSPreviewServiceRolePolicy

Description: Amazon RDS Preview Service Role Policy

AmazonRDSPreviewServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 31, 2018, 18:02 UTC
- **Edited time:** October 04, 2023, 19:01 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSReadOnlyAccess

Description: Provides read only access to Amazon RDS via the AWS Management Console.

AmazonRDSReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRDSReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** April 14, 2023, 12:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRDSServiceRolePolicy

Description: Allows Amazon RDS to manage AWS resources on your behalf.

AmazonRDSServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 08, 2018, 18:17 UTC
- **Edited time:** January 19, 2024, 15:10 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

Policy version

Policy version: v13 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftAllCommandsFullAccess

Description: This policy includes permissions to run SQL commands to copy, load, unload, query, and analyze data on Amazon Redshift. The policy also grants permissions to run select statements for related services, such as Amazon S3, Amazon CloudWatch logs, Amazon SageMaker, or AWS Glue.

AmazonRedshiftAllCommandsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftAllCommandsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 04, 2021, 00:48 UTC
- **Edited time:** November 25, 2021, 02:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftDataFullAccess

Description: This policy provides full access to Amazon Redshift Data APIs. This policy also grants scoped access to other required services.

AmazonRedshiftDataFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftDataFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 09, 2020, 19:23 UTC
- **Edited time:** April 07, 2023, 18:18 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
      }
    }
  ]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftFullAccess

Description: Provides full access to Amazon Redshift via the AWS Management Console.

AmazonRedshiftFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** July 07, 2022, 23:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftQueryEditor

Description: Provides full access to the Amazon Redshift Query Editor and to saved queries via the AWS Management Console.

AmazonRedshiftQueryEditor is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftQueryEditor to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 04, 2018, 22:50 UTC
- **Edited time:** February 16, 2021, 19:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftQueryEditorV2FullAccess

Description: Grants full access to the Amazon Redshift Query Editor V2 operations and resources. This policy also grants access to other required services. This includes permissions to list the Amazon Redshift clusters, read keys and aliases in AWS KMS and manage the Query Editor V2 secrets in AWS Secrets Manager.

AmazonRedshiftQueryEditorV2FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftQueryEditorV2FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 24, 2021, 14:06 UTC
- **Edited time:** February 21, 2024, 17:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftQueryEditorV2NoSharing

Description: Grants the ability to work with Amazon Redshift Query Editor V2 without sharing resources. The granted principal can only read, update and delete its own resources but cannot share them. This policy also grants access to other required services. This includes permissions to list the Amazon Redshift clusters and manage the Query Editor V2 secrets of the principal in AWS Secrets Manager.

AmazonRedshiftQueryEditorV2NoSharing is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftQueryEditorV2NoSharing to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 24, 2021, 14:18 UTC
- **Edited time:** February 21, 2024, 17:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
```

```
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "ResourceGroupsTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateFolder",
    "sqlworkbench:PutTab",
    "sqlworkbench:BatchDeleteFolder",
    "sqlworkbench>DeleteTab",
    "sqlworkbench:GenerateSession",
    "sqlworkbench:GetAccountInfo",
```

```

    "sqlworkbench:GetAccountSettings",
    "sqlworkbench:GetUserInfo",
    "sqlworkbench:GetUserWorkspaceSettings",
    "sqlworkbench:PutUserWorkspaceSettings",
    "sqlworkbench:ListConnections",
    "sqlworkbench:ListFiles",
    "sqlworkbench:ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench:ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench:ListTaggedResources",
    "sqlworkbench:ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench:ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench>DeleteChart",

```



```
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench>DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench>CreateNotebookCell",
    "sqlworkbench>DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench>CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
```

```
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : "sqlworkbench-resource-owner"
  },
  "StringEquals" : {
    "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
    "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
  }
}
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftQueryEditorV2ReadSharing

Description: Grants the ability to work with Amazon Redshift Query Editor V2 with limited sharing of resources. The granted principal can read, write and share its own resources. The granted principal can read the resources shared with its team but cannot update them. This policy also grants access to other required services. This includes permissions to list the Amazon Redshift clusters and manage the Query Editor V2 secrets of the principal in AWS Secrets Manager.

AmazonRedshiftQueryEditorV2ReadSharing is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftQueryEditorV2ReadSharing to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 24, 2021, 14:22 UTC

- **Edited time:** February 21, 2024, 17:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
    }
  }
}

```

```
}  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

Description: Grants the ability to work with Amazon Redshift Query Editor V2 with sharing of resources. The granted principal can read, write and share its own resources. The granted principal can read and update the resources shared with its team. This policy also grants access to other required services. This includes permissions to list the Amazon Redshift clusters and manage the Query Editor V2 secrets of the principal in AWS Secrets Manager.

AmazonRedshiftQueryEditorV2ReadWriteSharing is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftQueryEditorV2ReadWriteSharing to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 24, 2021, 14:25 UTC
- **Edited time:** February 21, 2024, 17:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
```

```

    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",
      "sqlworkbench>ListTabs",
      "sqlworkbench:UpdateFolder",
      "sqlworkbench>ListRedshiftClusters",
      "sqlworkbench:DriverExecute",
      "sqlworkbench>ListTaggedResources",
      "sqlworkbench>ListQueryExecutionHistory",
      "sqlworkbench:GetQueryExecutionHistory",
      "sqlworkbench>ListNotebooks",
      "sqlworkbench:GetSchemaInference",
      "sqlworkbench:GetAutocompletionMetadata",
      "sqlworkbench:GetAutocompletionResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateConnection",
      "sqlworkbench:CreateSavedQuery",
      "sqlworkbench:CreateChart",
      "sqlworkbench:CreateNotebook",
      "sqlworkbench:DuplicateNotebook",

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:DeleteChart",
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench>DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench>CreateNotebookCell",
    "sqlworkbench>DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench>CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
  ]
}

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-resource-owner"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:DuplicateNotebook",
  ]
}

```

```

    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:UntagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
}
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftReadOnlyAccess

Description: Provides read only access to Amazon Redshift via the AWS Management Console.

AmazonRedshiftReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRedshiftReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 08, 2024, 00:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRedshiftServiceLinkedRolePolicy

Description: Allows Amazon Redshift to call AWS services on your behalf

AmazonRedshiftServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 18, 2017, 19:19 UTC
- **Edited time:** March 15, 2024, 20:00 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Policy version

Policy version: v13 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    ]
}
]
}
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRekognitionCustomLabelsFullAccess

Description: This policy specifies rekognition and s3 permissions required by Amazon Rekognition Custom Labels feature.

AmazonRekognitionCustomLabelsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRekognitionCustomLabelsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 08, 2020, 19:18 UTC
- **Edited time:** August 16, 2022, 20:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRekognitionFullAccess

Description: Access to all Amazon Rekognition APIs

AmazonRekognitionFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRekognitionFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2016, 14:40 UTC
- **Edited time:** November 30, 2016, 14:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRekognitionReadOnlyAccess

Description: Access to all Read rekognition APIs

AmazonRekognitionReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRekognitionReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2016, 14:58 UTC
- **Edited time:** November 08, 2023, 18:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRekognitionServiceRole

Description: Allows Rekognition to call AWS services on your behalf.

AmazonRekognitionServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonRekognitionServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 29, 2017, 16:52 UTC
- **Edited time:** November 29, 2017, 16:52 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53AutoNamingFullAccess

Description: Provides full access to all Route 53 Auto Naming actions.

AmazonRoute53AutoNamingFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53AutoNamingFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 18, 2018, 18:40 UTC
- **Edited time:** January 18, 2018, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53AutoNamingReadOnlyAccess

Description: Provides read-only access to all Route 53 Auto Naming actions.

AmazonRoute53AutoNamingReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53AutoNamingReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 18, 2018, 03:02 UTC
- **Edited time:** January 18, 2018, 03:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53AutoNamingRegistrantAccess

Description: Provides registrant level access to Route 53 Auto Naming actions.

AmazonRoute53AutoNamingRegistrantAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonRoute53AutoNamingRegistrantAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 12, 2018, 22:33 UTC
- **Edited time:** March 12, 2018, 22:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53DomainsFullAccess

Description: Provides full access to all Route53 Domains actions and Create Hosted Zone to allow Hosted Zone creation as part of domain registrations.

AmazonRoute53DomainsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53DomainsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53DomainsReadOnlyAccess

Description: Provides access to Route53 Domains list and actions.

AmazonRoute53DomainsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53DomainsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53FullAccess

Description: Provides full access to all Amazon Route 53 via the AWS Management Console.

AmazonRoute53FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** December 20, 2018, 21:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53ProfilesFullAccess

Description: This policy grants full access to Amazon Route 53 Profile resources.

AmazonRoute53ProfilesFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53ProfilesFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 30, 2024, 18:30 UTC
- **Edited time:** April 30, 2024, 18:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53ProfilesReadOnlyAccess

Description: This policy grants read-only access to Amazon Route 53 Profile resources.

AmazonRoute53ProfilesReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53ProfilesReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 30, 2024, 18:29 UTC
- **Edited time:** April 30, 2024, 18:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53ReadOnlyAccess

Description: Provides read only access to all Amazon Route 53 via the AWS Management Console.

AmazonRoute53ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 15, 2016, 21:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ]
    }
  ],
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryClusterFullAccess

Description: Provides full access to Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53RecoveryClusterFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 18:37 UTC
- **Edited time:** August 18, 2021, 18:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

Description: Provides read only access to Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53RecoveryClusterReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 17:36 UTC
- **Edited time:** April 01, 2022, 17:37 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryControlConfigFullAccess

Description: Provides full access to Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonRoute53RecoveryControlConfigFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 17:48 UTC
- **Edited time:** August 18, 2021, 17:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Description: Provides read only access to Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53RecoveryControlConfigReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 18:01 UTC
- **Edited time:** October 18, 2023, 17:15 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryReadinessFullAccess

Description: Provides full access to Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53RecoveryReadinessFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 16:45 UTC

- **Edited time:** August 18, 2021, 16:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

Description: Provides read only access to Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonRoute53RecoveryReadinessReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 18, 2021, 18:11 UTC
- **Edited time:** November 09, 2021, 20:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",

```

```
    "route53-recovery-readiness:ListRules",
    "route53-recovery-readiness:ListTagsForResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53-recovery-readiness:GetArchitectureRecommendations",
    "route53-recovery-readiness:GetCellReadinessSummary"
  ],
  "Resource" : "arn:aws:route53-recovery-readiness::*:*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53ResolverFullAccess

Description: Full access policy for Route 53 Resolver

AmazonRoute53ResolverFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53ResolverFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 30, 2019, 18:10 UTC
- **Edited time:** July 17, 2020, 19:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonRoute53ResolverReadOnlyAccess

Description: Read only policy for Route 53 Resolver

AmazonRoute53ResolverReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonRoute53ResolverReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 30, 2019, 18:11 UTC
- **Edited time:** September 27, 2019, 16:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ]
    }
  ],
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonS3FullAccess

Description: Provides full access to all buckets via the AWS Management Console.

AmazonS3FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonS3FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** September 27, 2021, 20:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonS3FullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonS3ObjectLambdaExecutionRolePolicy

Description: Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants Lambda permissions to write to CloudWatch Logs.

AmazonS3ObjectLambdaExecutionRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonS3ObjectLambdaExecutionRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** August 18, 2021, 10:07 UTC
- **Edited time:** August 18, 2021, 10:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonS3OutpostsFullAccess

Description: Provides full access to Amazon S3 on Outposts via the AWS Management Console.

AmazonS3OutpostsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonS3OutpostsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 02, 2020, 17:26 UTC
- **Edited time:** October 02, 2020, 17:26 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonS3OutpostsReadOnlyAccess

Description: Provides read only access to Amazon S3 on Outposts via the AWS Management Console.

AmazonS3OutpostsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonS3OutpostsReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 02, 2020, 18:55 UTC
- **Edited time:** October 02, 2020, 18:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonS3ReadOnlyAccess

Description: Provides read only access to all buckets via the AWS Management Console.

AmazonS3ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonS3ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** August 10, 2023, 21:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Description: Service role policy used by the AWS service Catalog service to provision products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including CodePipeline, CodeBuild, CodeCommit, Glue, CloudFormation, etc,.

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2020, 18:48 UTC
- **Edited time:** July 01, 2024, 07:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

"Statement" : [
  {
    "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:PATCH",
      "apigateway:DELETE"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/sagemaker:launch-source" : "*"
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:POST"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "sagemaker:launch-source"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:PATCH"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:::/account"
    ]
  }
]

```

```
"Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
"Effect" : "Allow",
"Action" : [
  "cloudformation:CreateStack",
  "cloudformation:UpdateStack",
  "cloudformation>DeleteStack"
],
"Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
"Condition" : {
  "ArnLikeIfExists" : {
    "cloudformation:RoleArn" : [
      "arn:aws:sts:*:*:assumed-role/AmazonSageMakerServiceCatalog*"
    ]
  }
}
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false"
    }
  }
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
```

```
    "cloudformation:ValidateTemplate"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:UpdateProject"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:CreateCommit",
    "codecommit:CreateRepository",
    "codecommit>DeleteRepository",
    "codecommit:GetRepository",
    "codecommit:TagResource"
  ],
  "Resource" : [
    "arn:aws:codecommit:*:*:agemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:ListRepositories"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
  "Effect" : "Allow",
  "Action" : [
    "codepipeline:CreatePipeline",
    "codepipeline>DeletePipeline",
```



```

    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineState",
    "codepipeline:StartPipelineExecution",
    "codepipeline:TagResource",
    "codepipeline:UpdatePipeline"
  ],
  "Resource" : [
    "arn:aws:codepipeline:*:*:sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
  "Effect" : "Allow",
  "Action" : [
    "cognito-idp:CreateUserPool",
    "cognito-idp:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "sagemaker:launch-source"
      ]
    }
  }
},
{
  "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
  "Effect" : "Allow",
  "Action" : [
    "cognito-idp:CreateGroup",
    "cognito-idp:CreateUserPoolDomain",
    "cognito-idp:CreateUserPoolClient",
    "cognito-idp>DeleteGroup",
    "cognito-idp>DeleteUserPool",
    "cognito-idp>DeleteUserPoolClient",
    "cognito-idp>DeleteUserPoolDomain",
    "cognito-idp:DescribeUserPool",
    "cognito-idp:DescribeUserPoolClient",
    "cognito-idp:UpdateUserPool",
    "cognito-idp:UpdateUserPoolClient"
  ],
  "Resource" : "*",
  "Condition" : {

```

```
    "StringLike" : {
      "aws:ResourceTag/sagemaker:launch-source" : "*"
    }
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr:DeleteRepository",
      "ecr:TagResource"
    ],
    "Resource" : [
      "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events>DeleteRule",
      "events:DisableRule",
      "events:EnableRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
    "Effect" : "Allow",
    "Action" : [
      "firehose:CreateDeliveryStream",
      "firehose>DeleteDeliveryStream",
      "firehose:DescribeDeliveryStream",
      "firehose:StartDeliveryStreamEncryption",
      "firehose:StopDeliveryStreamEncryption",
      "firehose:UpdateDestination"
    ],
  },
```

```

    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateDatabase",
      "glue>DeleteDatabase"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/sagemaker-*",
      "arn:aws:glue:*:*:table/sagemaker-*",
      "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGlueClassifierPermission",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateClassifier",
      "glue>DeleteClassifier",
      "glue>DeleteCrawler",
      "glue>DeleteJob",
      "glue>DeleteTrigger",
      "glue>DeleteWorkflow",
      "glue:StopCrawler"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateWorkflow"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:workflow/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",

```

```
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateJob"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:job/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateCrawler",
      "glue:GetCrawler"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:crawler/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateTrigger",
      "glue:GetTrigger"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:trigger/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSageMakerServiceCatalog*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
    "Effect" : "Allow",
    "Action" : [
```

```

    "lambda:AddPermission",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction",
    "lambda:RemovePermission"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
  "Effect" : "Allow",
  "Action" : "lambda:TagResource",
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : [
        "sagemaker:*"
      ]
    }
  }
},
{
  "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogGroup",
    "logs>DeleteLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
    "arn:aws:logs:*:*:log-group::log-stream:*"
  ]
},

```

```
{
  "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
    }
  }
},
{
  "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : [
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteBucketPolicy",
    "s3:GetBucketPolicy",
    "s3:PutBucketAcl",
    "s3:PutBucketNotification",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketLogging",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketCORS",
    "s3:PutBucketTagging",
    "s3:PutObjectTagging"
  ],
  "Resource" : "arn:aws:s3:::sagemaker-*"
},
{
  "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateEndpoint",
```

```

    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateModel",
    "sagemaker:CreateWorkteam",
    "sagemaker>DeleteEndpoint",
    "sagemaker>DeleteEndpointConfig",
    "sagemaker>DeleteModel",
    "sagemaker>DeleteWorkteam",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeWorkteam",
    "sagemaker:CreateCodeRepository",
    "sagemaker:DescribeCodeRepository",
    "sagemaker:UpdateCodeRepository",
    "sagemaker>DeleteCodeRepository"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:*"
  ]
},
{
  "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:endpoint/*",
    "arn:aws:sagemaker:*:*:endpoint-config/*",
    "arn:aws:sagemaker:*:*:model/*",
    "arn:aws:sagemaker:*:*:pipeline/*",
    "arn:aws:sagemaker:*:*:project/*",
    "arn:aws:sagemaker:*:*:model-package*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : [
        "sagemaker:*"
      ]
    }
  }
},
{
  "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",

```

```

    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateImage",
      "sagemaker:DeleteImage",
      "sagemaker:DescribeImage",
      "sagemaker:UpdateImage",
      "sagemaker:ListTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:image/*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
    "Effect" : "Allow",
    "Action" : [
      "states:CreateStateMachine",
      "states>DeleteStateMachine",
      "states:UpdateStateMachine"
    ],
    "Resource" : [
      "arn:aws:states:*:*:stateMachine:sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
    "Effect" : "Allow",
    "Action" : "codestar-connections:PassConnection",
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
    "Condition" : {
      "StringEquals" : {
        "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
    "Effect" : "Allow",
    "Action" : "codeconnections:PassConnection",
    "Resource" : "arn:aws:codeconnections:*:*:connection/*",
    "Condition" : {
      "StringEquals" : {
        "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
      }
    }
  }
}

```



```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasAIServicesAccess

Description: Provides permissions for Amazon SageMaker Canvas to use AI services to support ready to use AI solutions. This policy will add more mutating permissions for services as Amazon SageMaker Canvas adds support.

AmazonSageMakerCanvasAIServicesAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasAIServicesAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 23, 2023, 22:36 UTC
- **Edited time:** November 29, 2023, 14:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
}

```

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasBedrockAccess

Description: This policy grants permissions to use Amazon Bedrock in SageMaker Canvas by providing access to downstream services such as S3.

AmazonSageMakerCanvasBedrockAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasBedrockAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 02, 2024, 18:37 UTC
- **Edited time:** February 02, 2024, 18:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasDataPrepFullAccess

Description: Provides full access to Amazon SageMaker resources and operations for data preparation in Canvas. The policy also provides select access to related services (e.g., S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue, EventBridge, Secrets Manager). This policy should be attached to the Amazon SageMaker Domain/User Profile execution role.

AmazonSageMakerCanvasDataPrepFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasDataPrepFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 27, 2023, 22:56 UTC
- **Edited time:** December 08, 2023, 02:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasDirectDeployAccess

Description: Allows Amazon SageMaker Canvas to create, manage and view endpoint details for endpoints created through Canvas. Allows Amazon SageMaker Canvas to retrieve endpoint invocation metrics from CloudWatch.

AmazonSageMakerCanvasDirectDeployAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasDirectDeployAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 06, 2023, 18:11 UTC
- **Edited time:** October 06, 2023, 18:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasForecastAccess

Description: This policy grants permissions commonly needed to use SageMaker Canvas with Amazon Forecast.

AmazonSageMakerCanvasForecastAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasForecastAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 24, 2022, 20:04 UTC
- **Edited time:** August 24, 2022, 20:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    ]
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCanvasFullAccess

Description: Provides full access to Amazon SageMaker Canvas resources and operations. The policy also provides select access to related services (e.g., S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager, and Forecast). This policy should be attached to the Amazon SageMaker Domain/User Profile execution role.

AmazonSageMakerCanvasFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerCanvasFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 09, 2022, 00:44 UTC
- **Edited time:** January 24, 2024, 22:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerClusterInstanceRolePolicy

Description: This policy grants permissions commonly needed to use Amazon SageMaker Cluster.

AmazonSageMakerClusterInstanceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerClusterInstanceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2023, 15:11 UTC
- **Edited time:** November 29, 2023, 15:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerCoreServiceRolePolicy

Description: Managed policy for Service Linked Role for Amazon SageMaker Core Services

AmazonSageMakerCoreServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 21, 2020, 21:40 UTC
- **Edited time:** December 21, 2020, 21:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerEdgeDeviceFleetPolicy

Description: Provides permissions necessary for SageMaker Edge to create and manage a device fleet for the customer using the default cloud connection.

AmazonSageMakerEdgeDeviceFleetPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerEdgeDeviceFleetPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 08, 2020, 16:17 UTC

- **Edited time:** December 08, 2020, 16:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        ]
      }
    }
  }
}

```

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerFeatureStoreAccess

Description: Provides permissions required to enable the offline store for an Amazon SageMaker FeatureStore feature group.

AmazonSageMakerFeatureStoreAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerFeatureStoreAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 16:24 UTC
- **Edited time:** December 05, 2022, 14:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerFullAccess

Description: Provides full access to Amazon SageMaker via the AWS Management Console and SDK. Also provides select access to related services (e.g., S3, ECR, CloudWatch Logs).

AmazonSageMakerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 13:07 UTC
- **Edited time:** March 29, 2024, 17:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

Policy version

Policy version: v26 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerGeospatialExecutionRole

Description: This policy provide access to services that are commonly needed to use SageMaker geospatial.

AmazonSageMakerGeospatialExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerGeospatialExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 30, 2022, 10:08 UTC
- **Edited time:** May 10, 2023, 20:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerGeospatialFullAccess

Description: This policy grants permissions that allow full access to Amazon SageMaker Geospatial through the AWS Management Console and SDK.

AmazonSageMakerGeospatialFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerGeospatialFullAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 30, 2022, 10:06 UTC
- **Edited time:** November 30, 2022, 10:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerGroundTruthExecution

Description: Provides access to AWS services that are required to run SageMaker GroundTruth Labeling job

AmazonSageMakerGroundTruthExecution is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerGroundTruthExecution to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2020, 19:30 UTC
- **Edited time:** April 29, 2022, 20:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerMechanicalTurkAccess

Description: Provides access to create Amazon Augmented AI FlowDefinition resources against any Workteam.

AmazonSageMakerMechanicalTurkAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerMechanicalTurkAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** December 03, 2019, 16:19 UTC
- **Edited time:** December 03, 2019, 16:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerModelGovernanceUseAccess

Description: This AWS managed policy grants permissions needed to use all Amazon SageMaker Governance features. The policy also provides select access to related services (e.g., S3, KMS).

AmazonSageMakerModelGovernanceUseAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerModelGovernanceUseAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2022, 08:58 UTC
- **Edited time:** June 04, 2024, 21:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerModelRegistryFullAccess

Description: This is a new managed policy for Model Registry in Sagemaker. This policy is a standalone policy that can be attached to the user role to access Model Registry related functionalities in Sagemaker.

AmazonSageMakerModelRegistryFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerModelRegistryFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 13, 2023, 05:20 UTC
- **Edited time:** June 06, 2024, 18:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerNotebooksServiceRolePolicy

Description: Managed policy for Service Linked Role for Amazon SageMaker Notebooks

AmazonSageMakerNotebooksServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 18, 2019, 20:27 UTC
- **Edited time:** May 22, 2024, 19:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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"
      }
    }
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

Description: Service role policy used by the AWS APIGateway within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including Lambda and others.

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 01, 2023, 15:06 UTC
- **Edited time:** August 01, 2023, 15:06 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationS

Description: Service role policy used by the AWS CloudFormation within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a subset of related services including Lambda, APIGateway and others.

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 01, 2023, 15:06 UTC
- **Edited time:** August 01, 2023, 15:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
        }
    }
}
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

Description: Service role policy used by the AWS Lambda within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including Secrets Manager and others.

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 01, 2023, 15:05 UTC
- **Edited time:** August 01, 2023, 15:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerPipelinesIntegrations

Description: This Amazon Managed Policy grants permissions commonly needed for use with Callback steps and Lambda steps in SageMaker Model Building Pipelines. It is added to the AmazonSageMaker-ExecutionRole that can be created when setting up SageMaker Studio. It can also be attached to any other role that will be used for authoring or executing pipelines.

AmazonSageMakerPipelinesIntegrations is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerPipelinesIntegrations to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 30, 2021, 16:35 UTC
- **Edited time:** February 17, 2023, 21:28 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerReadOnly

Description: Provides read only access to Amazon SageMaker via the AWS Management Console and SDK.

AmazonSageMakerReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 13:07 UTC
- **Edited time:** December 01, 2021, 16:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:ListGroup",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

Description: Service role policy used by the AWS APIGateway within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including CloudWatch Logs and others.

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 25, 2022, 04:25 UTC

- **Edited time:** March 25, 2022, 04:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

Description: Service role policy used by the AWS CloudFormation within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a subset of related services including SageMaker and others.

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 25, 2022, 04:26 UTC
- **Edited time:** March 25, 2022, 04:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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: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"
  ],
  "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"
  ]
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePol

Description: Service role policy used by the AWS CodeBuild within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a subset of related services including CodePipeline, CodeBuild and others.

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 25, 2022, 04:27 UTC
- **Edited time:** June 11, 2024, 18:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRole

Description: Service role policy used by the AWS CodePipeline within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a subset of related services including CodePipeline, CodeBuild and others.

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 22, 2022, 09:53 UTC
- **Edited time:** June 11, 2024, 18:37 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Description: Service role policy used by the AWS CloudWatch Events within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a subset of related services including CodePipeline and others.

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 22, 2022, 09:53 UTC
- **Edited time:** February 22, 2022, 09:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Description: Service role policy used by the AWS Firehose within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including Firehose and others.

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 22, 2022, 09:54 UTC
- **Edited time:** February 22, 2022, 09:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Description: Service role policy used by the AWS Glue within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including Glue, S3 and others.

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 22, 2022, 09:51 UTC
- **Edited time:** August 26, 2022, 19:13 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Description: Service role policy used by the AWS Lambda within the AWS ServiceCatalog provisioned products from Amazon SageMaker portfolio of products. Grants permissions to a set of related services including ECR, S3 and others.

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 04, 2022, 16:34 UTC
- **Edited time:** June 11, 2024, 18:57 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr>DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
```

```
"Effect" : "Allow",
"Action" : [
  "events:DeleteRule",
  "events:DescribeRule",
  "events:PutRule",
  "events:PutTargets",
  "events:RemoveTargets"
],
"Resource" : [
  "arn:aws:events:*:*:rule/sagemaker-*"
]
},
{
  "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3>ListAllMyBuckets",
    "s3>ListBucket",
    "s3>ListBucketMultipartUploads",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
}
```

```
]
},
{
  "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
    "sagemaker:CreateAction",
    "sagemaker:CreateAlgorithm",
    "sagemaker:CreateApp",
    "sagemaker:CreateAppImageConfig",
    "sagemaker:CreateArtifact",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateCodeRepository",
    "sagemaker:CreateCompilationJob",
    "sagemaker:CreateContext",
    "sagemaker:CreateDataQualityJobDefinition",
    "sagemaker:CreateDeviceFleet",
    "sagemaker:CreateDomain",
    "sagemaker:CreateEdgePackagingJob",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateExperiment",
    "sagemaker:CreateFeatureGroup",
    "sagemaker:CreateFlowDefinition",
    "sagemaker:CreateHumanTaskUi",
    "sagemaker:CreateHyperParameterTuningJob",
    "sagemaker:CreateImage",
    "sagemaker:CreateImageVersion",
    "sagemaker:CreateInferenceRecommendationsJob",
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateLineageGroupPolicy",
    "sagemaker:CreateModel",
    "sagemaker:CreateModelBiasJobDefinition",
    "sagemaker:CreateModelExplainabilityJobDefinition",
    "sagemaker:CreateModelPackage",
    "sagemaker:CreateModelPackageGroup",
    "sagemaker:CreateModelQualityJobDefinition",
```

```
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
"sagemaker>DeleteModelPackageGroup",
"sagemaker>DeleteModelPackageGroupPolicy",
"sagemaker>DeleteModelQualityJobDefinition",
"sagemaker>DeleteMonitoringSchedule",
```



```
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
```

```
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
```

```
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
```

```
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
```

```
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:action/*",
  "arn:aws:sagemaker:*:*:algorithm/*",
  "arn:aws:sagemaker:*:*:app-image-config/*",
  "arn:aws:sagemaker:*:*:artifact/*",
  "arn:aws:sagemaker:*:*:automl-job/*",
  "arn:aws:sagemaker:*:*:code-repository/*",
  "arn:aws:sagemaker:*:*:compilation-job/*",
  "arn:aws:sagemaker:*:*:context/*",
  "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
  "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
  "arn:aws:sagemaker:*:*:device-fleet/*",
  "arn:aws:sagemaker:*:*:edge-packaging-job/*",
  "arn:aws:sagemaker:*:*:endpoint/*",
  "arn:aws:sagemaker:*:*:endpoint-config/*",
  "arn:aws:sagemaker:*:*:experiment/*",
  "arn:aws:sagemaker:*:*:experiment-trial/*",
  "arn:aws:sagemaker:*:*:experiment-trial-component/*",
  "arn:aws:sagemaker:*:*:feature-group/*",
  "arn:aws:sagemaker:*:*:human-loop/*",
  "arn:aws:sagemaker:*:*:human-task-ui/*",
  "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
  "arn:aws:sagemaker:*:*:image/*",
  "arn:aws:sagemaker:*:*:image-version/*/*",
  "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
  "arn:aws:sagemaker:*:*:labeling-job/*",
  "arn:aws:sagemaker:*:*:model/*",
  "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
  "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
  "arn:aws:sagemaker:*:*:model-package/*",
  "arn:aws:sagemaker:*:*:model-package-group/*",
  "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
  "arn:aws:sagemaker:*:*:monitoring-schedule/*",
  "arn:aws:sagemaker:*:*:notebook-instance/*",
  "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
  "arn:aws:sagemaker:*:*:pipeline/*",
  "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
```

```

        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaPassRolePermission",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaLogPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs>DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs>ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}

```

```
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSecurityLakeAdministrator

Description: Provides full access to Amazon Security Lake and related services needed to administer Security Lake.

AmazonSecurityLakeAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AmazonSecurityLakeAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 30, 2023, 22:04 UTC

- **Edited time:** February 23, 2024, 16:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",

```



```

    "events:ListApiDestinations",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "kms:DescribeKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowManagingSecurityLakeS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketVersioning",
    "s3:PutReplicationConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetBucketNotification"
  ],
  "Resource" : "arn:aws:s3:::aws-security-data-lake*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowLambdaCreateFunction",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*"
  ]
}

```

```

    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowLambdaAddPermission",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    },
    "StringEquals" : {
      "lambda:Principal" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowGlueActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "glue:CreateTable",
    "glue:GetTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "AllowEventBridgeActions",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:PutRule",
    "events:DescribeRule",
    "events:CreateApiDestination",
    "events:CreateConnection",
    "events:UpdateConnection",
    "events:UpdateApiDestination",
    "events>DeleteConnection",
    "events>DeleteApiDestination",
    "events:ListTargetsByRule",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/AmazonSecurityLake*",
    "arn:aws:events:*:*:rule/SecurityLake*",
    "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
    "arn:aws:events:*:*:connection/AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowSQSActions",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs:SetQueueAttributes",
    "sqs:GetQueueURL",
    "sqs:AddPermission",
    "sqs:GetQueueAttributes",
    "sqs>DeleteQueue"
  ],
  "Resource" : [
```

```

    "arn:aws:sqs:*:*:SecurityLake*",
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowKmsCmkGrantForSecurityLake",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "GenerateDataKey",
        "RetireGrant",
        "Decrypt"
      ]
    }
  }
},
{
  "Sid" : "AllowEnablingQueryBasedSubscribers",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "ram:ResourceArn" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  }
}

```

```

    ]
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "securitylake.amazonaws.com"
  }
},
{
  "Sid" : "AllowConfiguringQueryBasedSubscribers",
  "Effect" : "Allow",
  "Action" : [
    "ram:UpdateResourceShare",
    "ram:GetResourceShares",
    "ram:DisassociateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:ResourceShareName" : "LakeFormation*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:PutSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",

```

```

    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      }
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",

```

```

    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "s3.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "s3.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:s3::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",

```

```

    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "events.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake::*:subscriber/*"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "events.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:events::*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  }
}

```



```

    }
  },
  {
    "Sid" : "AllowOnboardingToSecurityLakeDependencies",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinations.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AllowRolePolicyActionsforSubscribersandSources",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition" : {
      "StringEquals" : {
        "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {

```

```

    "Sid" : "AllowRegisterS3LocationInLakeFormation",
    "Effect" : "Allow",
    "Action" : [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowIAMActionsByResource",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRolePolicies",
      "iam>DeleteRole"
    ],
    "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3ReadAccessToSecurityLakes",
    "Effect" : "Allow",
    "Action" : [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
  },

```

```
    "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid" : "S3ResourcelessReadOnly",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSecurityLakeMetastoreManager

Description: Policy for Amazon SecurityLake meta store manager lambda which allows the access to cloudwatch, S3, Glue and SQS.

AmazonSecurityLakeMetastoreManager is an [AWS managed policy](#).

Using this policy

You can attach AmazonSecurityLakeMetastoreManager to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 23, 2024, 15:26 UTC
- **Edited time:** April 01, 2024, 20:04 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSecurityLakePermissionsBoundary

Description: Amazon Security Lake creates IAM roles for third-party custom sources to write data to a data lake and for third-party subscribers to consume data from a data lake, and uses this policy when creating these roles to define the boundary of their permissions.

AmazonSecurityLakePermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AmazonSecurityLakePermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2022, 14:11 UTC
- **Edited time:** May 14, 2024, 20:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSESFullAccess

Description: Provides full access to Amazon SES via the AWS Management Console.

AmazonSESFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSESFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSESEFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSESReadOnlyAccess

Description: Provides read only access to Amazon SES via the AWS Management Console.

AmazonSESReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSESReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** May 14, 2024, 12:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}  
 ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSESServiceRolePolicy

Description: Allows SES to publish Amazon CloudWatch basic monitoring metrics on behalf of your SES resources

AmazonSESServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 21, 2024, 16:02 UTC
- **Edited time:** May 21, 2024, 16:02 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSNSFullAccess

Description: Provides full access to Amazon SNS via the AWS Management Console.

AmazonSNSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSNSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSNSReadOnlyAccess

Description: Provides read only access to Amazon SNS via the AWS Management Console.

AmazonSNSReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSNSReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSNSRole

Description: Default policy for Amazon SNS service role.

AmazonSNSRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonSNSRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSNSRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents",
  "logs:PutMetricFilter",
  "logs:PutRetentionPolicy"
],
"Resource" : [
  "*"
]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSQSFullAccess

Description: Provides full access to Amazon SQS via the AWS Management Console.

AmazonSQSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSQSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSQSFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSQSReadOnlyAccess

Description: Provides read only access to Amazon SQS via the AWS Management Console.

AmazonSQSReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSQSReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** May 24, 2024, 18:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMAutomationApproverAccess

Description: Provides access to view automation executions and send approval decisions to automation waiting for approval

AmazonSSMAutomationApproverAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMAutomationApproverAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 07, 2017, 23:07 UTC
- **Edited time:** August 07, 2017, 23:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeAutomationExecutions",
      "ssm:GetAutomationExecution",
      "ssm:SendAutomationSignal"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMAutomationRole

Description: Provides permissions for EC2 Automation service to execute activities defined within Automation documents

AmazonSSMAutomationRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMAutomationRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 05, 2016, 22:09 UTC
- **Edited time:** July 24, 2017, 23:29 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMDirectoryServiceAccess

Description: This policy allows SSM Agent to access Directory Service on behalf of the customer for domain-join the managed instance.

AmazonSSMDirectoryServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonSSMDirectoryServiceAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 15, 2019, 17:44 UTC
- **Edited time:** March 15, 2019, 17:44 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMFullAccess

Description: Provides full access to Amazon SSM.

AmazonSSMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 29, 2015, 17:39 UTC
- **Edited time:** November 20, 2019, 20:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSSMFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMMaintenanceWindowRole

Description: Service Role to be used for EC2 Maintenance Window

AmazonSSMMaintenanceWindowRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMMaintenanceWindowRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2016, 15:57 UTC
- **Edited time:** July 27, 2019, 00:16 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

    "ssm:GetParameters",
    "ssm:ListCommands",
    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SSM*",
    "arn:aws:lambda:*:*:function:*:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states:DescribeExecution",
    "states:StartExecution"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:SSM*",
    "arn:aws:states:*:*:execution:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:ListGroup",
    "resource-groups:ListGroupResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ]
}

```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

Description: This policy enables AWS Systems Manager functionality on EC2 instances.

AmazonSSMManagedEC2InstanceDefaultPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMManagedEC2InstanceDefaultPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 30, 2022, 20:54 UTC
- **Edited time:** August 30, 2022, 20:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMManagedInstanceCore

Description: The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.

AmazonSSMManagedInstanceCore is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMManagedInstanceCore to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 15, 2019, 17:22 UTC
- **Edited time:** May 23, 2019, 16:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMPatchAssociation

Description: Provide access to child instances for patch association operation.

AmazonSSMPatchAssociation is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMPatchAssociation to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 13, 2020, 16:00 UTC
- **Edited time:** May 13, 2020, 16:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMReadOnlyAccess

Description: Provides read only access to Amazon SSM.

AmazonSSMReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSSMReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 29, 2015, 17:44 UTC
- **Edited time:** May 29, 2015, 17:44 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSSMServiceRolePolicy

Description: Provides access to AWS Resources managed or used by Amazon SSM

AmazonSSMServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 13, 2017, 19:20 UTC
- **Edited time:** September 14, 2022, 19:46 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonSumerianFullAccess

Description: Provides full access to Amazon Sumerian.

AmazonSumerianFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonSumerianFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 24, 2018, 20:14 UTC
- **Edited time:** April 24, 2018, 20:14 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonSumerianFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "sumerian:*"
  ],
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTextextractFullAccess

Description: Access to all Amazon Textract APIs

AmazonTextextractFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTextextractFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 19:07 UTC
- **Edited time:** November 28, 2018, 19:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTextextractFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTextractServiceRole

Description: Allows Textract to call AWS services on your behalf.

AmazonTextractServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AmazonTextractServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** November 28, 2018, 19:12 UTC
- **Edited time:** November 28, 2018, 19:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AmazonTextextractServiceRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTimestreamConsoleFullAccess

Description: Provides full access to manage Amazon Timestream using the AWS Management Console. Note that this policy also grants permissions for certain KMS operations, and operations

to manage your saved queries. If using Customer managed CMK, please refer to documentation for additional permissions needed.

AmazonTimestreamConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTimestreamConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 30, 2020, 21:47 UTC
- **Edited time:** February 01, 2022, 21:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTimestreamFullAccess

Description: Provides full access to Amazon Timestream. Note that this policy also grants certain KMS operation access. If using Customer managed CMK, please refer to documentation for additional permissions needed.

AmazonTimestreamFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTimestreamFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 30, 2020, 21:47 UTC
- **Edited time:** November 26, 2021, 23:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTimestreamInfluxDBFullAccess

Description: Provides full administrative access to create, update, delete and list Amazon Timestream InfluxDB instances and create and list parameter groups. Please refer to documentation for additional permissions needed.

AmazonTimestreamInfluxDBFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTimestreamInfluxDBFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 14, 2024, 22:53 UTC
- **Edited time:** March 14, 2024, 22:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTimestreamInfluxDBServiceRolePolicy

Description: Provides full administrative access to create, update, delete and list Amazon Timestream InfluxDB instances and create and list parameter groups. Please refer to documentation for additional permissions needed.

AmazonTimestreamInfluxDBServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 14, 2024, 18:53 UTC
- **Edited time:** March 14, 2024, 18:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTimestreamReadOnlyAccess

Description: Provides read only access to Amazon Timestream. Policy also provides permission to cancel any running query. If using Customer managed CMK, please refer to documentation for additional permissions needed.

AmazonTimestreamReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTimestreamReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** September 30, 2020, 21:47 UTC
- **Edited time:** June 05, 2024, 19:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTranscribeFullAccess

Description: Provides full access to Amazon Transcribe operations

AmazonTranscribeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTranscribeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 04, 2018, 16:06 UTC
- **Edited time:** April 04, 2018, 16:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "transcribe:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*transcribe*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonTranscribeReadOnlyAccess

Description: Provides access to read only operation for Amazon Transcribe

AmazonTranscribeReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonTranscribeReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 04, 2018, 16:05 UTC

- **Edited time:** April 04, 2018, 16:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

Description: Provides access to create network interfaces and attach them to cross-account resources

AmazonVPCCrossAccountNetworkInterfaceOperations is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCCrossAccountNetworkInterfaceOperations to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 18, 2017, 20:47 UTC
- **Edited time:** September 25, 2023, 15:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCFullAccess

Description: Provides full access to Amazon VPC via the AWS Management Console.

AmazonVPCFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 08, 2024, 16:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonVPCFullAccess

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Description: Provides permissions to describe AWS resources, run Network Access Analyzer, and create or delete tags on Network Insights Access Scope and Network Insights Access Scope Analysis.

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCNetworkAccessAnalyzerFullAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 15, 2023, 22:56 UTC
- **Edited time:** May 15, 2024, 21:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Description: Provides permissions to describe AWS resources, run Reachability Analyzer, and create or delete tags on Network Insights Path and Network Insights Analysis.

AmazonVPCReachabilityAnalyzerFullAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCReachabilityAnalyzerFullAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 14, 2023, 20:12 UTC
- **Edited time:** May 15, 2024, 20:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Action" : [
  "directconnect:DescribeConnections",
  "directconnect:DescribeDirectConnectGatewayAssociations",
  "directconnect:DescribeDirectConnectGatewayAttachments",
  "directconnect:DescribeDirectConnectGateways",
  "directconnect:DescribeVirtualGateways",
  "directconnect:DescribeVirtualInterfaces"
],
"Resource" : "*"
},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInsightsPath",
    "ec2>DeleteNetworkInsightsAnalysis",
    "ec2>DeleteNetworkInsightsPath",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAnalyses",
    "ec2:DescribeNetworkInsightsPaths",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
```

```

    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAnalysis"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2TagsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-path/*",
    "arn:*:ec2:*:*:network-insights-analysis/*"
  ]
},
{
  "Sid" : "ElasticloadbalancingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GlobalacceleratorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",

```

```
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "Sid" : "NetworkFirewallPermissions",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TirosPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Description: This policy is attached to the role IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. This role is deployed to the member accounts in an organization when the management account enables trusted access for Reachability Analyzer. It provides permissions to view resources from across your organization using the Reachability Analyzer console.

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCReachabilityAnalyzerPathComponentReadPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 01, 2023, 20:38 UTC
- **Edited time:** May 01, 2023, 20:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Effect" : "Allow",
    "Action" : [
      "network-firewall:Describe*",
      "network-firewall:List*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonVPCReadOnlyAccess

Description: Provides read only access to Amazon VPC via the AWS Management Console.

AmazonVPCReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonVPCReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 08, 2024, 17:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkDocsFullAccess

Description: Provides full access to Amazon WorkDocs via the AWS Management Console

AmazonWorkDocsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkDocsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 16, 2020, 23:05 UTC
- **Edited time:** April 16, 2020, 23:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkDocsReadOnlyAccess

Description: Provides read only access to Amazon WorkDocs via the AWS Management Console

AmazonWorkDocsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonWorkDocsReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 08, 2020, 23:49 UTC
- **Edited time:** January 08, 2020, 23:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkMailEventsServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Amazon WorkMail Events

AmazonWorkMailEventsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 16, 2019, 16:52 UTC
- **Edited time:** April 16, 2019, 16:52 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkMailFullAccess

Description: Provides full access to WorkMail, Directory Service, SES, EC2 and read access to KMS metadata.

AmazonWorkMailFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkMailFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** December 21, 2020, 14:13 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkMailMessageFlowFullAccess

Description: Full access to the WorkMail Message Flow APIs

AmazonWorkMailMessageFlowFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkMailMessageFlowFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 11, 2021, 11:08 UTC
- **Edited time:** February 11, 2021, 11:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkMailMessageFlowReadOnlyAccess

Description: Read only access to WorkMail messages for the GetRawMessageContent API

AmazonWorkMailMessageFlowReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkMailMessageFlowReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 28, 2021, 12:40 UTC
- **Edited time:** January 28, 2021, 12:40 UTC

- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkMailReadOnlyAccess

Description: Provides read only access to WorkMail and SES.

AmazonWorkMailReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AmazonWorkMailReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** July 25, 2019, 08:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesAdmin

Description: Provides access to Amazon WorkSpaces administrative actions via AWS SDK and CLI.

AmazonWorkSpacesAdmin is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesAdmin to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 22, 2015, 22:21 UTC
- **Edited time:** June 27, 2024, 17:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces>DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ]
    }
  ]
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesApplicationManagerAdminAccess

Description: Provides administrator access for packaging an application in Amazon WorkSpaces Application Manager.

AmazonWorkSpacesApplicationManagerAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesApplicationManagerAdminAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 09, 2015, 14:03 UTC
- **Edited time:** April 09, 2015, 14:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkspacesPCAAccess

Description: This managed policy provides full administrative access to AWS Certificate Manager Private CA resources in your AWS account for certificate-based authentication.

AmazonWorkspacesPCAAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkspacesPCAAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 08, 2022, 00:25 UTC

- **Edited time:** November 08, 2022, 00:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesPoolServiceAccess

Description: This policy provides AWS WorkSpaces service access to required customer account resources for launching Workspaces Pools

AmazonWorkSpacesPoolServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesPoolServiceAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2024, 16:21 UTC
- **Edited time:** June 27, 2024, 16:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
```



```

    "ec2:DescribeRouteTables",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "WorkSpacesPoolS3Permissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:PutObject",
    "s3>DeleteObject",
    "s3:GetObjectVersion",
    "s3>DeleteObjectVersion",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutEncryptionConfiguration"
  ],
  "Resource" : [
    "arn:aws:s3:::wspool-logs-*",
    "arn:aws:s3:::wspool-app-settings-*",
    "arn:aws:s3:::wspool-home-folder-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesSecureBrowserReadOnly

Description: Provides read-only access to Amazon WorkSpaces Secure Browser and its dependencies through the AWS Management Console, SDK, and CLI.

AmazonWorkSpacesSecureBrowserReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesSecureBrowserReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2024, 20:01 UTC
- **Edited time:** June 24, 2024, 20:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
```

```

    "workspaces-web:GetIdentityProvider",
    "workspaces-web:GetNetworkSettings",
    "workspaces-web:GetPortal",
    "workspaces-web:GetPortalServiceProviderMetadata",
    "workspaces-web:GetTrustStore",
    "workspaces-web:GetTrustStoreCertificate",
    "workspaces-web:GetUserSettings",
    "workspaces-web:GetUserAccessLoggingSettings",
    "workspaces-web:GetIpAccessSettings",
    "workspaces-web:ListBrowserSettings",
    "workspaces-web:ListIdentityProviders",
    "workspaces-web:ListNetworkSettings",
    "workspaces-web:ListPortals",
    "workspaces-web:ListTagsForResource",
    "workspaces-web:ListTrustStoreCertificates",
    "workspaces-web:ListTrustStores",
    "workspaces-web:ListUserSettings",
    "workspaces-web:ListUserAccessLoggingSettings",
    "workspaces-web:ListIpAccessSettings"
  ],
  "Resource" : "arn:aws:workspaces-web:*:*:*"
},
{
  "Sid" : "Dependencies",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "kinesis:ListStreams"
  ],
  "Resource" : "*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesSelfServiceAccess

Description: Provides access to Amazon WorkSpaces backend service to perform Workspace Self Service actions

AmazonWorkSpacesSelfServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesSelfServiceAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2019, 19:22 UTC
- **Edited time:** June 27, 2019, 19:22 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesServiceAccess

Description: Provides customer account access to AWS WorkSpaces service for launching a Workspace.

AmazonWorkSpacesServiceAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesServiceAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2019, 19:19 UTC
- **Edited time:** March 18, 2020, 23:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesWebReadOnly

Description: Provides read-only access to Amazon WorkSpaces Web and its dependencies through the AWS Management Console, SDK, and CLI.

AmazonWorkSpacesWebReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AmazonWorkSpacesWebReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2021, 14:20 UTC

- **Edited time:** November 02, 2022, 20:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonWorkSpacesWebServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Amazon WorkSpaces Web

AmazonWorkSpacesWebServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 30, 2021, 13:15 UTC
- **Edited time:** December 15, 2022, 22:46 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonZocaloFullAccess

Description: Provides full access to Amazon Zocalo.

AmazonZocaloFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonZocaloFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AmazonZocaloFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmazonZocaloReadOnlyAccess

Description: Provides read only access to Amazon Zocalo

AmazonZocaloReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AmazonZocaloReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AmplifyBackendDeployFullAccess

Description: Provides Amplify full access permissions to deploy Amplify backend resources (AWS AppSync, Amazon Cognito, Amazon S3 and other related services) via the AWS Cloud Development Kit (AWS CDK)

AmplifyBackendDeployFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AmplifyBackendDeployFullAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 06, 2023, 21:32 UTC
- **Edited time:** May 31, 2024, 15:53 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

APIGatewayServiceRolePolicy

Description: Allows API Gateway to manage associated AWS Resources on behalf of the customer.

APIGatewayServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 20, 2017, 17:23 UTC
- **Edited time:** July 12, 2021, 22:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AppIntegrationsServiceLinkedRolePolicy

Description: Allows AppIntegrations to manage AppFlow resources and publish CloudWatch metric data on your behalf.

AppIntegrationsServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 30, 2022, 19:42 UTC
- **Edited time:** September 30, 2022, 19:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ApplicationAutoScalingForAmazonAppStreamAccess

Description: Policy to enable Application Autoscaling for Amazon AppStream

ApplicationAutoScalingForAmazonAppStreamAccess is an [AWS managed policy](#).

Using this policy

You can attach ApplicationAutoScalingForAmazonAppStreamAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2017, 21:39 UTC
- **Edited time:** February 06, 2017, 21:39 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Application Discovery Service Continuous Export feature

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 09, 2018, 20:22 UTC
- **Edited time:** August 13, 2018, 22:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AppRunnerNetworkingServiceRolePolicy

Description: Allows AWS AppRunner Networking to manage related AWS resources on your behalf.

AppRunnerNetworkingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 12, 2022, 21:02 UTC
- **Edited time:** January 12, 2022, 21:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AppRunnerServiceRolePolicy

Description: Allows AWS AppRunner to manage related AWS resources on your behalf.

AppRunnerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 14, 2021, 19:15 UTC
- **Edited time:** May 14, 2021, 19:15 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingConsoleFullAccess

Description: Provides full access to Auto Scaling via the AWS Management Console.

AutoScalingConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AutoScalingConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2017, 19:43 UTC
- **Edited time:** February 06, 2018, 23:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingConsoleReadOnlyAccess

Description: Provides read-only access to Auto Scaling via the AWS Management Console.

AutoScalingConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AutoScalingConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2017, 19:48 UTC
- **Edited time:** January 12, 2017, 19:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingFullAccess

Description: Provides full access to Auto Scaling.

AutoScalingFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AutoScalingFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2017, 19:31 UTC
- **Edited time:** February 06, 2018, 21:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AutoScalingFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingNotificationAccessRole

Description: Default policy for the AutoScaling Notification Access service role.

AutoScalingNotificationAccessRole is an [AWS managed policy](#).

Using this policy

You can attach AutoScalingNotificationAccessRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingReadOnlyAccess

Description: Provides read-only access to Auto Scaling.

AutoScalingReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AutoScalingReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2017, 19:39 UTC
- **Edited time:** January 12, 2017, 19:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AutoScalingServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Auto Scaling

AutoScalingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 08, 2018, 23:10 UTC
- **Edited time:** February 29, 2024, 17:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS_ConfigRole

Description: Default policy for AWS Config service role. Provides permissions required for AWS Config to track changes to your AWS resources.

AWS_ConfigRole is an [AWS managed policy](#).

Using this policy

You can attach AWS_ConfigRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 15, 2020, 20:30 UTC

- **Edited time:** June 17, 2024, 18:58 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

Policy version

Policy version: v31 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
"emr-containers: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",
"redshift:DescribeTags",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"rekognition:DescribeStreamProcessor",
"rekognition:ListStreamProcessors",
```

```
"rekognition:ListTagsForResource",
"resiliencyhub:DescribeApp",
"resiliencyhub:DescribeAppVersionTemplate",
"resiliencyhub:DescribeResiliencyPolicy",
"resiliencyhub:ListApps",
"resiliencyhub:ListAppVersionResourceMappings",
"resiliencyhub:ListResiliencyPolicies",
"resiliencyhub: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",
"ssm-sap: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/*"
}
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAccountActivityAccess

Description: Allows users to access the Account Activity page.

AWSAccountActivityAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAccountActivityAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** March 07, 2023, 17:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAccountActivityAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAccountManagementFullAccess

Description: Provides full access to AWS Account Management.

AWSAccountManagementFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSAccountManagementFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 30, 2021, 23:20 UTC
- **Edited time:** September 30, 2021, 23:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAccountManagementReadOnlyAccess

Description: Provides read-only access to AWS Account Management

AWSAccountManagementReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAccountManagementReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 30, 2021, 23:29 UTC
- **Edited time:** September 30, 2021, 23:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAccountUsageReportAccess

Description: Allows users to access the Account Usage Report page.

AWSAccountUsageReportAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAccountUsageReportAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "aws-portal:ViewUsage"
  ],
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAgentlessDiscoveryService

Description: Provides access for the Discovery Agentless Connector to register with AWS Application Discovery Service.

AWSAgentlessDiscoveryService is an [AWS managed policy](#).

Using this policy

You can attach AWSAgentlessDiscoveryService to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 02, 2016, 01:35 UTC
- **Edited time:** February 24, 2020, 23:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppFabricFullAccess

Description: Provides full access to the AWS AppFabric service and read only access to dependent services such as S3, Kinesis, KMS.

AWSAppFabricFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppFabricFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2023, 19:51 UTC
- **Edited time:** June 27, 2023, 19:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppFabricFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppFabricReadOnlyAccess

Description: Provides read only access to the AWS AppFabric

AWSAppFabricReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppFabricReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2023, 19:52 UTC
- **Edited time:** June 27, 2023, 19:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppFabricServiceRolePolicy

Description: Provides AppFabric access to AWS resources on your behalf

AWSAppFabricServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 26, 2023, 21:07 UTC
- **Edited time:** June 26, 2023, 21:07 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

Description: Policy granting permissions to Application Auto Scaling to access AppStream and CloudWatch.

AWSApplicationAutoscalingAppStreamFleetPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 20, 2017, 19:04 UTC
- **Edited time:** October 20, 2017, 19:04 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingCassandraTablePolicy

Description: Policy granting permissions to Application Auto Scaling to access Cassandra and CloudWatch.

AWSApplicationAutoscalingCassandraTablePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 18, 2020, 22:49 UTC
- **Edited time:** March 18, 2020, 22:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

Description: Policy granting permissions to Application Auto Scaling to access Comprehend and CloudWatch.

AWSApplicationAutoscalingComprehendEndpointPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 14, 2019, 18:39 UTC
- **Edited time:** November 14, 2019, 18:39 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoScalingCustomResourcePolicy

Description: Policy granting permissions to Application Auto Scaling to access APIGateway and CloudWatch for custom resource scaling

AWSApplicationAutoScalingCustomResourcePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 04, 2018, 23:22 UTC
- **Edited time:** June 04, 2018, 23:22 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "execute-api:Invoke",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

Description: Policy granting permissions to Application Auto Scaling to access DynamoDB and CloudWatch.

AWSApplicationAutoscalingDynamoDBTablePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 20, 2017, 21:34 UTC
- **Edited time:** October 20, 2017, 21:34 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Description: Policy granting permissions to Application Auto Scaling to access EC2 Spot Fleet and CloudWatch.

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 25, 2017, 18:23 UTC
- **Edited time:** October 25, 2017, 18:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingECSServicePolicy

Description: Policy granting permissions to Application Auto Scaling to access EC2 Container Service and CloudWatch.

AWSApplicationAutoscalingECSServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 25, 2017, 23:53 UTC
- **Edited time:** October 25, 2017, 23:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

Description: Policy granting permissions to Application Auto Scaling to access Amazon ElastiCache and Amazon CloudWatch.

AWSApplicationAutoscalingElastiCacheRGPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 17, 2021, 23:41 UTC
- **Edited time:** August 17, 2021, 23:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElasticCacheRGPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Description: Policy granting permissions to Application Auto Scaling to access Elastic Map Reduce and CloudWatch.

AWSApplicationAutoscalingEMRInstanceGroupPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 26, 2017, 00:57 UTC
- **Edited time:** October 26, 2017, 00:57 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingKafkaClusterPolicy

Description: Policy granting permissions to Application Auto Scaling to access Managed Streaming for Apache Kafka and CloudWatch.

AWSApplicationAutoscalingKafkaClusterPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 24, 2020, 18:36 UTC
- **Edited time:** August 24, 2020, 18:36 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```


Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Description: Policy granting permissions to Application Auto Scaling to access Lambda and CloudWatch.

AWSApplicationAutoscalingLambdaConcurrencyPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 21, 2019, 20:04 UTC
- **Edited time:** October 21, 2019, 20:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:PutProvisionedConcurrencyConfig",
      "lambda:GetProvisionedConcurrencyConfig",
      "lambda>DeleteProvisionedConcurrencyConfig",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

Description: Policy granting permissions to Application Auto Scaling to access Amazon Neptune and Amazon CloudWatch.

AWSApplicationAutoscalingNeptuneClusterPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 02, 2021, 21:14 UTC

- **Edited time:** September 02, 2021, 21:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingRDSClusterPolicy

Description: Policy granting permissions to Application Auto Scaling to access RDS and CloudWatch.

AWSApplicationAutoscalingRDSClusterPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 17, 2017, 17:46 UTC
- **Edited time:** August 07, 2018, 19:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

Description: Policy granting permissions to Application Auto Scaling to access SageMaker and CloudWatch.

AWSApplicationAutoscalingSageMakerEndpointPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 06, 2018, 19:58 UTC
- **Edited time:** November 13, 2023, 18:52 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Description: Policy granting permissions to Application Auto Scaling to access Amazon WorkSpaces and Amazon CloudWatch.

AWSApplicationAutoscalingWorkSpacesPoolPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 17, 2024, 18:39 UTC
- **Edited time:** June 17, 2024, 18:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationDiscoveryAgentAccess

Description: Provides access for the Discovery Agent to register with AWS Application Discovery Service.

AWSApplicationDiscoveryAgentAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationDiscoveryAgentAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2016, 21:38 UTC

- **Edited time:** February 24, 2020, 22:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

Description: Allows Application Discovery Service Agentless Collectors to auto update, register, and communicate with Application Discovery Service

AWSApplicationDiscoveryAgentlessCollectorAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationDiscoveryAgentlessCollectorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 16, 2022, 21:00 UTC
- **Edited time:** August 16, 2022, 21:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationDiscoveryServiceFullAccess

Description: Provides full access to view and tag Configuration Items maintained by the AWS Application Discovery Service

AWSApplicationDiscoveryServiceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationDiscoveryServiceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2016, 21:30 UTC
- **Edited time:** June 19, 2019, 21:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationAgentInstallationPolicy

Description: This policy allows installing the AWS Replication Agent, which is used with AWS Application Migration Service (MGN) to migrate external servers to AWS. Attach this policy to your IAM users or roles whose credentials you provide when installing the AWS Replication Agent.

AWSApplicationMigrationAgentInstallationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationAgentInstallationPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 19, 2022, 07:51 UTC
- **Edited time:** September 20, 2022, 11:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationAgentPolicy

Description: This policy allows installing and using the AWS Replication Agent, which is used with AWS Application Migration Service (MGN) to migrate external servers to AWS. Attach this policy to your IAM users or roles whose credentials you provide when installing the AWS Replication Agent.

AWSApplicationMigrationAgentPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationAgentPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 07, 2021, 07:00 UTC
- **Edited time:** September 20, 2022, 11:13 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationAgentPolicy_v2

Description: This policy allows using the AWS Replication Agent, which is used with AWS Application Migration Service (MGN) to migrate external servers to AWS. We do not recommend that you attach this policy to your IAM users or roles.

AWSApplicationMigrationAgentPolicy_v2 is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationAgentPolicy_v2 to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 06, 2022, 14:14 UTC
- **Edited time:** June 06, 2022, 14:14 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationConversionServerPolicy

Description: This policy allows the Application Migration Service (MGN) Conversion Server, which are EC2 instances launched by Application Migration Service, to communicate with the MGN service. An IAM role with this policy is attached (as an EC2 Instance Profile) by MGN to the MGN Conversion Servers, which are automatically launched and terminated by MGN, when needed. We do not recommend that you attach this policy to your IAM users or roles. MGN Conversion Servers are used by Application Migration Service when users choose to launch Test or Cutover instances using the MGN console, CLI, or API.

AWSApplicationMigrationConversionServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationConversionServerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 07, 2021, 06:48 UTC
- **Edited time:** April 07, 2021, 06:48 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationEC2Access

Description: This policy provides Amazon EC2 operations required to use Application Migration Service (MGN) to launch the migrated servers as EC2 instances. Attach this policy to your IAM users or roles.

AWSApplicationMigrationEC2Access is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationEC2Access to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 07, 2021, 07:05 UTC
- **Edited time:** February 06, 2023, 16:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationFullAccess

Description: This policy provides permissions to all public APIs of AWS Application Migration Service (MGN), as well as permissions to read KMS key information. Attach this policy to your IAM users or roles.

AWSApplicationMigrationFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 07, 2021, 06:56 UTC
- **Edited time:** May 19, 2024, 08:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationMGHAccess

Description: This policy allows AWS Application Migration Service (MGN) to send meta-data about the progress of servers being migrated using MGN to AWS Migration Hub (MGH). MGN automatically creates an IAM role with this policy attached, and assumes this role. We do not recommend that you attach this policy to your IAM users or roles.

AWSApplicationMigrationMGHAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationMGHAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 07, 2021, 07:10 UTC

- **Edited time:** April 07, 2021, 07:10 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationReadOnlyAccess

Description: This policy provides permissions to all read-only public APIs of Application Migration Service (MGN), as well as some read-only APIs of other AWS services that are required in order to make full read-only use of the MGN console. Attach this policy to your IAM users or roles.

AWSApplicationMigrationReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 07, 2021, 07:15 UTC
- **Edited time:** March 20, 2023, 08:58 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationReplicationServerPolicy

Description: This policy allows the Application Migration Service (MGN) Replication Servers, which are EC2 instances launched by Application Migration Service - to communicate with the MGN service, and to create EBS snapshots in your AWS account. An IAM role with this policy is attached (as an EC2 Instance Profile) by Application Migration Service to the MGN Replication Servers which are automatically launched and terminated by MGN, as needed. MGN Replication Servers are used to facilitate data replication from your external servers to AWS, as part of the migration process managed using MGN. We do not recommend that you attach this policy to your IAM users or roles.

AWSApplicationMigrationReplicationServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationReplicationServerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 07, 2021, 07:21 UTC
- **Edited time:** April 07, 2021, 07:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationServiceEc2InstancePolicy

Description: This policy allows installing and using the AWS Replication Agent, which is used by AWS Application Migration Service (AWS MGN) to migrate source servers that run on EC2 (cross-Region or cross-AZ). An IAM role with this policy should be attached (as an EC2 Instance Profile) to the EC2 Instances.

AWSApplicationMigrationServiceEc2InstancePolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSApplicationMigrationServiceEc2InstancePolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 22, 2023, 13:19 UTC
- **Edited time:** January 03, 2024, 14:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationServiceRolePolicy

Description: Allows AWS application Migration Service to create and manage AWS resources on your behalf.

AWSApplicationMigrationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 07, 2021, 06:43 UTC
- **Edited time:** June 20, 2023, 09:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationSSMAccess

Description: This policy provides access to Amazon SSM operations required to use Application Migration Service (MGN) to execute custom post migration command SSM documents. Attach this policy to your IAM users or roles.

AWSApplicationMigrationSSMAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationSSMAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 09:29 UTC
- **Edited time:** March 20, 2023, 10:57 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSApplicationMigrationVCenterClientPolicy

Description: This policy allows installing and using the AWS VCenter Client, which is used with AWS Application Migration Service (MGN) to migrate external servers to AWS. Attach this policy to your IAM users or roles whose credentials you provide when installing the AWS VCenter Client.

AWSApplicationMigrationVCenterClientPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSApplicationMigrationVCenterClientPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 08, 2021, 12:53 UTC
- **Edited time:** November 08, 2021, 12:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshEnvoyAccess

Description: App Mesh Envoy policy for accessing Virtual Node configuration.

AWSAppMeshEnvoyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppMeshEnvoyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 03, 2019, 21:29 UTC
- **Edited time:** July 03, 2019, 21:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshFullAccess

Description: Provides full access to the AWS App Mesh APIs and Management Console.

AWSAppMeshFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppMeshFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 16, 2019, 17:50 UTC
- **Edited time:** January 07, 2021, 19:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppMeshFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshPreviewEnvoyAccess

Description: App Mesh Preview Envoy policy for accessing Virtual Node configuration.

AWSAppMeshPreviewEnvoyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppMeshPreviewEnvoyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 05, 2019, 23:32 UTC
- **Edited time:** August 05, 2019, 23:32 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshPreviewServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by AWS App Mesh

AWSAppMeshPreviewServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 19, 2019, 19:07 UTC
- **Edited time:** August 21, 2019, 21:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
    }
  ]
}
```



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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshReadOnly

Description: Provides read-only access to the AWS App Mesh APIs and Management Console.

AWSAppMeshReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSAppMeshReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 16, 2019, 17:51 UTC
- **Edited time:** January 07, 2021, 19:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppMeshReadOnly

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppMeshServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by AWS AppMesh

AWSAppMeshServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 03, 2019, 18:30 UTC
- **Edited time:** October 10, 2023, 16:46 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:DiscoverInstances",
      "servicediscovery:DiscoverInstancesRevision"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ACMCertificateVerification",
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppRunnerFullAccess

Description: Grants permissions to all App Runner actions.

AWSAppRunnerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppRunnerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 11, 2022, 04:02 UTC
- **Edited time:** January 11, 2022, 04:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppRunnerReadOnlyAccess

Description: Grants permissions to list and view details about App Runner resources.

AWSAppRunnerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppRunnerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 24, 2022, 21:24 UTC
- **Edited time:** February 24, 2022, 21:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "apprunner:List*",
      "apprunner:Describe*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppRunnerServicePolicyForECRAccess

Description: AWS App Runner service policy that grants read permissions to Amazon ECR resources in the customer's account. Use it in a role that is passed to App Runner when creating or updating an App Runner service.

AWSAppRunnerServicePolicyForECRAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppRunnerServicePolicyForECRAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 14, 2021, 19:17 UTC
- **Edited time:** May 14, 2021, 19:17 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppSyncAdministrator

Description: Provides administrative access to the AppSync service, though not enough to access via the console.

AWSAppSyncAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AWSAppSyncAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 20, 2018, 21:20 UTC
- **Edited time:** November 04, 2019, 19:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppSyncAdministrator

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppSyncInvokeFullAccess

Description: Provides full invoking access to the AppSync service - both through the console and independently

AWSAppSyncInvokeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAppSyncInvokeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 20, 2018, 21:21 UTC
- **Edited time:** March 20, 2018, 21:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppSyncPushToCloudWatchLogs

Description: Allows AppSync to push logs to user's CloudWatch account.

AWSAppSyncPushToCloudWatchLogs is an [AWS managed policy](#).

Using this policy

You can attach AWSAppSyncPushToCloudWatchLogs to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 09, 2018, 19:38 UTC
- **Edited time:** April 09, 2018, 19:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppSyncSchemaAuthor

Description: Provides access to create, update, and query the schema.

AWSAppSyncSchemaAuthor is an [AWS managed policy](#).

Using this policy

You can attach AWSAppSyncSchemaAuthor to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 20, 2018, 21:21 UTC
- **Edited time:** February 01, 2023, 18:36 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAppSyncServiceRolePolicy

Description: Enables access to AWS services and resources used or managed by AppSync

AWSAppSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 21, 2020, 19:56 UTC
- **Edited time:** January 21, 2020, 19:56 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSArtifactAccountSync

Description: Allows AWS Artifact read-only access to operations in AWS Organizations.

AWSArtifactAccountSync is an [AWS managed policy](#).

Using this policy

You can attach AWSArtifactAccountSync to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 10, 2018, 23:04 UTC

- **Edited time:** April 10, 2018, 23:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSArtifactReportsReadOnlyAccess

Description: Provides read-only access to the AWS Artifact service reports.

AWSArtifactReportsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSArtifactReportsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 02, 2024, 22:42 UTC
- **Edited time:** January 02, 2024, 22:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSArtifactServiceRolePolicy

Description: Allows AWS Artifact to gather information about an organization via AWS Organizations service.

AWSArtifactServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 21, 2023, 20:27 UTC
- **Edited time:** August 21, 2023, 20:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAuditManagerAdministratorAccess

Description: Provides administrative access to enable or disable AWS Audit Manager, update settings, and manage assessments, controls, and frameworks

AWSAuditManagerAdministratorAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSAuditManagerAdministratorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 11, 2020, 20:02 UTC
- **Edited time:** May 15, 2024, 23:46 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAuditManagerServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by AWS Audit Manager

AWSAuditManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 08, 2020, 15:12 UTC
- **Edited time:** June 10, 2024, 20:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

Description: Policy granting permissions to AWS Auto Scaling to periodically forecast capacity and generate scheduled scaling actions for Auto Scaling groups in a scaling plan

AWSAutoScalingPlansEC2AutoScalingPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 23, 2018, 22:46 UTC
- **Edited time:** August 23, 2018, 22:46 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
```

```
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupAuditAccess

Description: This policy grants permissions for users to create controls and frameworks that define their expectations for AWS Backup resources and activities, and to audit AWS Backup resources and activities against their defined controls and frameworks. This policy grants permissions to AWS Config and similar services to describe user expectations perform the audits. This policy also grants permissions to deliver audit reports to S3 and similar services, and enables users to find and open their audit reports.

AWSBackupAuditAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupAuditAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 24, 2021, 01:02 UTC
- **Edited time:** April 10, 2023, 21:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBackupAuditAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupDataTransferAccess

Description: This policy allows the AWS Backint agent to complete backup data transfer with AWS Backup Storage plane. Attach this policy to roles assumed by EC2 Instances running SAP HANA with the Backint agent.

AWSBackupDataTransferAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupDataTransferAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 10, 2022, 22:48 UTC
- **Edited time:** November 10, 2022, 22:48 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupFullAccess

Description: This policy is for backup administrators, granting full access to AWS Backup operations, including creating or editing backup plans, assigning AWS resources to backup plans, deleting backups, and restoring backups.

AWSBackupFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 18, 2019, 22:21 UTC
- **Edited time:** November 27, 2023, 17:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Policy version

Policy version: v17 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
```

```
"Effect" : "Allow",
"Action" : "backup-storage:*",
"Resource" : "*"
},
{
  "Sid" : "RdsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBSnapshots",
    "rds:ListTagsForResource",
    "rds:DescribeDBInstances",
    "rds:describeDBEngineVersions",
    "rds:describeOptionGroups",
    "rds:describeOrderableDBInstanceOptions",
    "rds:describeDBSubnetGroups",
    "rds:describeDBClusterSnapshots",
    "rds:describeDBClusters",
    "rds:describeDBParameterGroups",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RdsDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds>DeleteDBSnapshot",
    "rds>DeleteDBClusterSnapshot"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DynamoDbPermissions",
  "Effect" : "Allow",
  "Action" : [
```

```
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DynamoDbDeleteBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DeleteBackup"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "EfsFileSystemPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFilesystems"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "Sid" : "Ec2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:describeAvailabilityZones",
    "ec2:DescribeVpcs",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeVpcEndpoints",
```



```
    "ec2:DescribeAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2DeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ResourceGroupTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "StorageGatewayVolumePermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeCachediSCSIVolumes",
    "storagegateway:DescribeStorediSCSIVolumes"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
},
{
  "Sid" : "StorageGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:ListGateways"
  ]
}
```

```

    ],
    "Resource" : "arn:aws:storagegateway:*:*:*"
  },
  {
    "Sid" : "StorageGatewayGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeGatewayInformation",
      "storagegateway:ListVolumes",
      "storagegateway:ListLocalDisks"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
  },
  {
    "Sid" : "IamRolePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles",
      "iam:GetRole"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IamPassRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/*AwsBackup*",
      "arn:aws:iam:*:*:role/*AWSBackup*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "backup.amazonaws.com",
          "restore-testing.backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AwsOrganizationsPermissions",
    "Effect" : "Allow",
    "Action" : "organizations:DescribeOrganization",
    "Resource" : "*"
  }

```

```
  },
  {
    "Sid" : "KmsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantPermissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      },
      "StringLike" : {
        "kms:ViaService" : "backup.*.amazonaws.com"
      }
    }
  }
},
{
  "Sid" : "SystemManagerCommandPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SystemManagerSendCommandPermissions",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
```

```

    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Sid" : "FsxPermissions",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems",
      "fsx:DescribeBackups",
      "fsx:DescribeVolumes",
      "fsx:DescribeStorageVirtualMachines"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "FsxDeletePermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DeleteBackup",
    "Resource" : "arn:aws:fsx:*:*:backup/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "DirectoryServicePermissions",
    "Effect" : "Allow",
    "Action" : "ds:DescribeDirectories",
    "Resource" : "*"
  },
  {
    "Sid" : "IamCreateServiceLinkedRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "backup.amazonaws.com",

```

```
        "restore-testing.backup.amazonaws.com"
    ]
}
},
{
  "Sid" : "BackupGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:AssociateGatewayToServer",
    "backup-gateway:CreateGateway",
    "backup-gateway>DeleteGateway",
    "backup-gateway>DeleteHypervisor",
    "backup-gateway:DisassociateGatewayFromServer",
    "backup-gateway:ImportHypervisorConfiguration",
    "backup-gateway:ListGateways",
    "backup-gateway:ListHypervisors",
    "backup-gateway:ListTagsForResource",
    "backup-gateway:ListVirtualMachines",
    "backup-gateway:PutMaintenanceStartTime",
    "backup-gateway:TagResource",
    "backup-gateway:TestHypervisorConfiguration",
    "backup-gateway:UntagResource",
    "backup-gateway:UpdateGatewayInformation",
    "backup-gateway:UpdateHypervisor"
  ],
  "Resource" : "*"
},
{
  "Sid" : "BackupGatewayHypervisorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:GetHypervisor",
    "backup-gateway:GetHypervisorPropertyMappings",
    "backup-gateway:PutHypervisorPropertyMappings",
    "backup-gateway:StartVirtualMachinesMetadataSync"
  ],
  "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
},
{
  "Sid" : "BackupGatewayVirtualMachinePermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:GetVirtualMachine"
```

```
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  },
  {
    "Sid" : "BackupGatewayGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetBandwidthRateLimitSchedule",
      "backup-gateway:GetGateway",
      "backup-gateway:PutBandwidthRateLimitSchedule"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
  },
  {
    "Sid" : "CloudWatchPermissions",
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  },
  {
    "Sid" : "TimestreamDatabasePermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:ListTables",
      "timestream:ListDatabases"
    ],
    "Resource" : [
      "arn:aws:timestream:*:*:database/*"
    ]
  },
  {
    "Sid" : "TimestreamPermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3BucketPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ]
  },
  ],
```

```
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Sid" : "RedshiftResourcesPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters",
      "redshift:DescribeClusterSubnetGroups",
      "redshift:DescribeClusterSnapshots",
      "redshift:DescribeSnapshotSchedules"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:cluster:*",
      "arn:aws:redshift:*:*:subnetgroup:*",
      "arn:aws:redshift:*:*:snapshot:*/*",
      "arn:aws:redshift:*:*:snapshotschedule:*"
    ]
  },
  {
    "Sid" : "RedshiftPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeNodeConfigurationOptions",
      "redshift:DescribeOrderableClusterOptions",
      "redshift:DescribeClusterParameterGroups",
      "redshift:DescribeClusterTracks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudFormationStackPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/*"
    ]
  },
  {
    "Sid" : "SystemsManagerForSapPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:GetOperation",
```

```
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ResourceAccessManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ram:GetResourceShareAssociations"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Description: Provides AWS BackupGateway permission to sync the metadata of Virtual Machines on your behalf

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** December 15, 2022, 19:43 UTC
- **Edited time:** December 15, 2022, 19:43 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupOperatorAccess

Description: This policy grants users permissions to assign AWS resources to backup plans, create on-demand backups, and restore backups. This policy does not allow the user to create or edit backup plans or to delete scheduled backups after they are created.

AWSBackupOperatorAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupOperatorAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 18, 2019, 22:23 UTC
- **Edited time:** September 06, 2023, 20:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Policy version

Policy version: v15 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupOrganizationAdminAccess

Description: This policy is for backup administrators who use cross-account backup management to manage backups for the organization.

AWSBackupOrganizationAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSBackupOrganizationAdminAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2020, 16:23 UTC
- **Edited time:** November 18, 2022, 18:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupRestoreAccessForSAPHANA

Description: Provides AWS Backup permission to restore a backup of SAP HANA on Amazon EC2

AWSBackupRestoreAccessForSAPHANA is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupRestoreAccessForSAPHANA to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 10, 2022, 22:43 UTC
- **Edited time:** November 10, 2022, 22:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceLinkedRolePolicyForBackup

Description: Provides AWS Backup permission to create backups on your behalf across AWS services

AWSBackupServiceLinkedRolePolicyForBackup is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 02, 2020, 23:08 UTC
- **Edited time:** May 17, 2024, 17:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Policy version

Policy version: v16 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CopySnapshot"
      }
    }
  },
  {
    "Sid" : "EC2CreateBackupTagPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*::image/*",
      "arn:aws:ec2:*::snapshot/*"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AWSBackupManagedResource"
        ]
      }
    }
  },
  {
    "Sid" : "EC2CreateTagsPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*::image/*",
      "arn:aws:ec2:*::snapshot/*"
    ],
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  },
  {
    "Sid" : "EC2RDSDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeSnapshotTierStatus",
      "ec2:DescribeImages",
      "rds:DescribeDBSnapshots",
```



```
    "rds:DescribeDBClusterSnapshots"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EBSCopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
  "Resource" : "arn:aws:ec2:*::snapshot/*"
},
{
  "Sid" : "EC2CopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopyImage",
  "Resource" : "*"
},
{
  "Sid" : "EC2ModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeregisterImage",
    "ec2>DeleteSnapshot",
    "ec2:ModifySnapshotTier"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSBackupManagedResource" : "false"
    }
  }
},
{
  "Sid" : "RDSInstanceAndSnapshotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:CopyDBSnapshot",
    "rds>DeleteDBSnapshot",
    "rds>DeleteDBInstanceAutomatedBackup"
  ],
  "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
},
{
  "Sid" : "RDSClusterPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "rds:AddTagsToResource",
  "rds:CopyDBClusterSnapshot",
  "rds>DeleteDBClusterSnapshot"
],
"Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
},
{
  "Sid" : "KMSDescribePermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSGrantPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListGrants",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "fsx.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : [
```

```
        "ec2.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "fsx.*.amazonaws.com"
    ]
}
},
{
    "Sid" : "FsxPermissions",
    "Effect" : "Allow",
    "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx>DeleteBackup"
    ],
    "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
    "Sid" : "DynamoDBDeletePermissions",
    "Effect" : "Allow",
    "Action" : "dynamodb>DeleteBackup",
    "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
},
{
    "Sid" : "BackupGateway",
    "Effect" : "Allow",
    "Action" : [
        "backup-gateway>ListVirtualMachines"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ListTagsForBackupGateway",
    "Effect" : "Allow",
    "Action" : [
        "backup-gateway>ListTagsForResource"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
},
{
    "Sid" : "DynamoDBPermissions",
    "Effect" : "Allow",
    "Action" : [
```

```

        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
    ],
    "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
    "Sid" : "StorageGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
},
{
    "Sid" : "EventBridgePermissions",
    "Effect" : "Allow",
    "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
    ],
    "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
    ]
},
{
    "Sid" : "EventBridgeRulesPermissions",
    "Effect" : "Allow",
    "Action" : "events:ListRules",
    "Resource" : "*"
},
{
    "Sid" : "SSMSAPPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
    ],

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "TimestreamResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:ListDatabases",
      "timestream:ListTables",
      "timestream:ListTagsForResource",
      "timestream:DescribeDatabase",
      "timestream:DescribeTable",
      "timestream:GetAwsBackupStatus",
      "timestream:GetAwsRestoreStatus"
    ],
    "Resource" : [
      "arn:aws:timestream:*:*:database/*"
    ]
  },
  {
    "Sid" : "TimestreamPermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RedshiftDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusterSnapshots",
      "redshift:DescribeTags"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:snapshot:*/*",
      "arn:aws:redshift:*:*:cluster:*"
    ]
  },
  {
    "Sid" : "RedshiftClusterSnapshotPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift>DeleteClusterSnapshot"
    ],
  },
```

```

    "Resource" : [
      "arn:aws:redshift:*:*:snapshot:*/*"
    ]
  },
  {
    "Sid" : "RedshiftClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:cluster:*"
    ]
  },
  {
    "Sid" : "CloudformationStackPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/*"
    ]
  },
  {
    "Sid" : "RecoveryPointTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup:TagResource"
    ],
    "Resource" : "arn:aws:backup:*:*:recovery-point:*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

Description: Provides AWS Backup permission to create backups on your behalf across AWS services

AWSBackupServiceLinkedRolePolicyForBackupTest is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 12, 2020, 17:37 UTC
- **Edited time:** May 12, 2020, 17:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceRolePolicyForBackup

Description: Provides AWS Backup permission to create backups on your behalf across AWS services

AWSBackupServiceRolePolicyForBackup is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupServiceRolePolicyForBackup to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 10, 2019, 21:01 UTC
- **Edited time:** May 17, 2024, 17:12 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Policy version

Policy version: v19 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb>DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds>CreateDBSnapshot",

```

```

        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
    ],
    "Resource" : "*"
},
{
    "Sid" : "RDSModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rds:ModifyDBInstance"
    ],
    "Resource" : [
        "arn:aws:rds:*:*:db:*"
    ]
},
{
    "Sid" : "RDSClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rds:ModifyDBCluster"
    ],
    "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
    ]
},
{
    "Sid" : "RDSClusterBackupPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rds>DeleteDBClusterAutomatedBackup"
    ],
    "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
},
{
    "Sid" : "RDSBackupPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rds>DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
    ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:rds:*:*:snapshot:awsbackup:*"
    ]
  },
  {
    "Sid" : "RDSClusterModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:DeleteDBClusterSnapshot",
      "rds:ModifyDBClusterSnapshotAttribute"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    ]
  },
  {
    "Sid" : "StorageGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:CreateSnapshot",
      "storagegateway:ListTagsForResource"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "EBSCopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopySnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopyImage"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EBSTagAndDeletePermissions",
    "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Sid" : "EC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateImage",
      "ec2:DeregisterImage",
      "ec2:DescribeSnapshots",
      "ec2:DescribeTags",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceCreditSpecifications",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeElasticGpus",
      "ec2:DescribeSpotInstanceRequests",
      "ec2:DescribeSnapshotTierStatus"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2TagPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:image/*"
  },
  {
    "Sid" : "EC2ModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2:ModifyImageAttribute"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/aws:backup:source-resource" : "false"
      }
    }
  }

```

```
    }
  }
},
{
  "Sid" : "EBSSnapshotTierPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotTier"
  ],
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "BackupVaultPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:DescribeBackupVault",
    "backup:CopyIntoBackupVault"
  ],
  "Resource" : "arn:aws:backup:*:*:backup-vault:*"
},
{
  "Sid" : "BackupVaultCopyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:CopyFromBackupVault"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EFSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:Backup",
    "elasticfilesystem:DescribeTags"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "Sid" : "EBSResourcePermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateSnapshot",
  "ec2>DeleteSnapshot",
  "ec2:DescribeVolumes",
  "ec2:DescribeSnapshots"
],
"Resource" : [
  "arn:aws:ec2:*::snapshot/*",
  "arn:aws:ec2:*:*:volume/*"
]
},
{
  "Sid" : "KMSDynamoDBPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "dynamodb.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSPermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
}
```

```
  },
  {
    "Sid" : "KMSDataKeyEC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "ec2.*.amazonaws.com"
        ]
      }
    }
  }
},
{
  "Sid" : "GetResourcesPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMSendPermissions",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Sid" : "FsxB BackupPermissions",
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceRolePolicyForRestores

Description: Provides AWS Backup permission to perform restores on your behalf across AWS services. This policy includes permissions to create and delete AWS resources, such as EBS volumes, RDS instances, and EFS file systems, which are part of the restore process.

AWSBackupServiceRolePolicyForRestores is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupServiceRolePolicyForRestores to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 12, 2019, 00:23 UTC
- **Edited time:** December 15, 2023, 22:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Policy version

Policy version: v20 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceRolePolicyForS3Backup

Description: Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This includes read access to all S3 objects and any decrypt access for all KMS keys.

AWSBackupServiceRolePolicyForS3Backup is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupServiceRolePolicyForS3Backup to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 18, 2022, 17:40 UTC
- **Edited time:** May 17, 2024, 17:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBackupServiceRolePolicyForS3Restore

Description: Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This includes read/write permissions to all S3 buckets, and permissions to GenerateDataKey and DescribeKey for all KMS keys.

AWSBackupServiceRolePolicyForS3Restore is an [AWS managed policy](#).

Using this policy

You can attach AWSBackupServiceRolePolicyForS3Restore to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 18, 2022, 17:39 UTC
- **Edited time:** February 07, 2023, 00:06 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBatchFullAccess

Description: Provides full access for AWS Batch resources.

AWSBatchFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBatchFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 06, 2016, 19:35 UTC

- **Edited time:** October 24, 2022, 16:09 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBatchFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBatchServiceEventTargetRole

Description: Policy to enable CloudWatch Event Target for AWS Batch Job Submission

AWSBatchServiceEventTargetRole is an [AWS managed policy](#).

Using this policy

You can attach AWSBatchServiceEventTargetRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 28, 2018, 22:31 UTC
- **Edited time:** February 28, 2018, 22:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBatchServiceRole

Description: Policy for AWS Batch service role which allows access to related services including EC2, Autoscaling, EC2 Container service and Cloudwatch Logs.

AWSBatchServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AWSBatchServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 06, 2016, 19:36 UTC
- **Edited time:** December 05, 2023, 18:49 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

Policy version

Policy version: v13 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBCMDDataExportsServiceRolePolicy

Description: A service linked role to provide Billing and Cost Management Data Exports access to AWS service data for exporting the data to a target location, such as Amazon S3, on behalf of a customer.

AWSBCMDDataExportsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 10, 2024, 17:40 UTC
- **Edited time:** June 10, 2024, 17:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDDataExportsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Sid" : "CostOptimizationRecommendationAccess",
    "Effect" : "Allow",
    "Action" : [
      "cost-optimization-hub:ListEnrollmentStatuses",
      "cost-optimization-hub:ListRecommendations"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBillingConductorFullAccess

Description: Use the AWSBillingConductorFullAccess managed policy to allow complete access to AWS Billing Conductor (ABC) console and APIs. This policy allows users to list, create and delete ABC resources.

AWSBillingConductorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBillingConductorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 13, 2022, 18:02 UTC
- **Edited time:** April 13, 2022, 18:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBillingConductorReadOnlyAccess

Description: Use the AWSBillingConductorReadOnlyAccess managed policy to allow read only access to AWS Billing Conductor (ABC) console and APIs. This policy grants permission to view and list all ABC resources. It does not include the ability to create or delete resources.

AWSBillingConductorReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBillingConductorReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 13, 2022, 18:02 UTC
- **Edited time:** April 13, 2022, 18:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBillingReadOnlyAccess

Description: Allows users to view bills on the Billing Console.

AWSBillingReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBillingReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 27, 2020, 20:08 UTC
- **Edited time:** May 23, 2024, 23:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Description: This policy gives permissions to control AWS resources. For example, to start and stop EC2 or RDS instances by executing AWS Systems Manager (SSM) scripts.

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM is an [AWS managed policy](#).

Using this policy

You can attach AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 25, 2022, 19:03 UTC
- **Edited time:** May 25, 2022, 19:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBudgetsActionsWithAWSResourceControlAccess

Description: Provides full access to AWS Budgets Actions including using Budgets Actions to control states of running AWS resources via AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBudgetsActionsWithAWSResourceControlAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 15, 2020, 17:19 UTC
- **Edited time:** October 15, 2020, 17:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBudgetsReadOnlyAccess

Description: Provides read only access to AWS Budgets Console via the AWS Management Console.

AWSBudgetsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBudgetsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 15, 2020, 17:18 UTC
- **Edited time:** June 17, 2024, 17:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBugBustFullAccess

Description: This IAM policy grants users full access to the AWS BugBust console

AWSBugBustFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBugBustFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** June 24, 2021, 07:03 UTC
- **Edited time:** July 22, 2021, 20:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBugBustFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBugBustPlayerAccess

Description: This IAM policy grants users access to participate in AWS BugBust events

AWSBugBustPlayerAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSBugBustPlayerAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2021, 07:15 UTC

- **Edited time:** June 24, 2021, 07:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSBugBustServiceRolePolicy

Description: Grants permissions to AWS BugBust to access resources on your behalf

AWSBugBustServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 24, 2021, 06:59 UTC
- **Edited time:** June 24, 2021, 06:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerFullAccess

Description: Provides full access to AWS Certificate Manager (ACM)

AWSCertificateManagerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSCertificateManagerFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 21, 2016, 17:02 UTC
- **Edited time:** August 17, 2020, 22:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerPrivateCAAuditor

Description: Provides auditor access to AWS Certificate Manager Private Certificate Authority

AWSCertificateManagerPrivateCAAuditor is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerPrivateCAAuditor to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 23, 2018, 16:51 UTC
- **Edited time:** August 17, 2020, 22:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerPrivateCAFullAccess

Description: Provides full access to AWS Certificate Manager Private Certificate Authority

AWSCertificateManagerPrivateCAFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerPrivateCAFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 23, 2018, 16:54 UTC
- **Edited time:** October 23, 2018, 16:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    "acm-pca:*"  
  ],  
  "Resource" : "*"   
}   
]   
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerPrivateCAPrivilegedUser

Description: Provides privileged certificate user access to AWS Certificate Manager Private Certificate Authority

AWSCertificateManagerPrivateCAPrivilegedUser is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerPrivateCAPrivilegedUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 20, 2019, 17:43 UTC
- **Edited time:** June 20, 2019, 17:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerPrivateCAReadOnly

Description: Provides read only access to AWS Certificate Manager Private Certificate Authority

AWSCertificateManagerPrivateCAReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerPrivateCAReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 23, 2018, 16:57 UTC
- **Edited time:** August 17, 2020, 22:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerPrivateCAUser

Description: Provides certificate user access to AWS Certificate Manager Private Certificate Authority

AWSCertificateManagerPrivateCAUser is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerPrivateCAUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 23, 2018, 16:53 UTC
- **Edited time:** June 20, 2019, 17:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCertificateManagerReadOnly

Description: Provides read only access to AWS Certificate Manager (ACM).

AWSCertificateManagerReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSCertificateManagerReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 21, 2016, 17:07 UTC
- **Edited time:** March 15, 2021, 16:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
```

```
    "acm:ListTagsForCertificate",
    "acm:GetAccountConfiguration"
  ],
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSChatbotServiceLinkedRolePolicy

Description: The Service Linked Role used by AWS Chatbot.

AWSChatbotServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 18, 2019, 16:39 UTC
- **Edited time:** November 18, 2019, 16:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCleanRoomsFullAccess

Description: Allows full access to AWS Clean Rooms resources and access to related AWS services.

AWSCleanRoomsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCleanRoomsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2023, 16:10 UTC
- **Edited time:** March 21, 2024, 15:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCleanRoomsFullAccessNoQuerying

Description: Allows full access to AWS Clean Rooms resources except for querying in a collaboration and access to related AWS services.

AWSCleanRoomsFullAccessNoQuerying is an [AWS managed policy](#).

Using this policy

You can attach AWSCleanRoomsFullAccessNoQuerying to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2023, 16:12 UTC
- **Edited time:** May 14, 2024, 18:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCleanRoomsMLFullAccess

Description: Allows full access to AWS Clean Rooms ML resources and access to related AWS services.

AWSCleanRoomsMLFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCleanRoomsMLFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2023, 21:02 UTC
- **Edited time:** November 29, 2023, 21:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCleanRoomsMLReadOnlyAccess

Description: Allows read-only access to AWS Clean Rooms ML resources and read-only access to related AWS Clean Rooms resources

AWSCleanRoomsMLReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCleanRoomsMLReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2023, 20:55 UTC
- **Edited time:** November 29, 2023, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCleanRoomsReadOnlyAccess

Description: Allows read-only access to AWS Clean Rooms resources and read-only access to related AWS Glue and Amazon CloudWatch Logs resources.

AWSCleanRoomsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCleanRoomsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 12, 2023, 16:10 UTC
- **Edited time:** January 12, 2023, 16:10 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloud9Administrator

Description: Provides administrator access to AWS Cloud9.

AWSCloud9Administrator is an [AWS managed policy](#).

Using this policy

You can attach AWSCloud9Administrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:17 UTC
- **Edited time:** October 11, 2023, 12:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloud9Administrator

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloud9EnvironmentMember

Description: Provides the ability to be invited into AWS Cloud9 shared development environments.

AWSCloud9EnvironmentMember is an [AWS managed policy](#).

Using this policy

You can attach AWSCloud9EnvironmentMember to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:18 UTC
- **Edited time:** October 11, 2023, 12:13 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloud9ServiceRolePolicy

Description: Service Linked Role Policy for AWS Cloud9

AWSCloud9ServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** November 30, 2017, 13:44 UTC
- **Edited time:** January 17, 2022, 14:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloud9SSMInstanceProfile

Description: This policy will be used to attach a role on a InstanceProfile which will allow Cloud9 to use the SSM Session Manager to connect to the instance

AWSCloud9SSMInstanceProfile is an [AWS managed policy](#).

Using this policy

You can attach `AWSCloud9SSMInstanceProfile` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 14, 2020, 11:40 UTC
- **Edited time:** May 14, 2020, 11:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloud9User

Description: Provides permission to create AWS Cloud9 development environments and to manage owned environments.

AWSCloud9User is an [AWS managed policy](#).

Using this policy

You can attach AWSCloud9User to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2017, 16:16 UTC
- **Edited time:** October 11, 2023, 13:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloud9User

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudFormationFullAccess

Description: Provides full access to AWS CloudFormation.

AWSCloudFormationFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudFormationFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 26, 2019, 21:50 UTC
- **Edited time:** July 26, 2019, 21:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudFormationFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudFormationReadOnlyAccess

Description: Provides access to AWS CloudFormation via the AWS Management Console.

AWSCloudFormationReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudFormationReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** November 13, 2019, 17:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS CloudFront Logger

Description: Grants CloudFront Logger write permissions to CloudWatch Logs.

AWSCloudFrontLogger is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 12, 2018, 20:15 UTC
- **Edited time:** November 22, 2019, 19:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudHSMFullAccess

Description: Provides full access to all CloudHSM resources.

AWSCloudHSMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudHSMFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** February 06, 2015, 18:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudHSMReadOnlyAccess

Description: Provides read only access to all CloudHSM resources.

AWSCloudHSMReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudHSMReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** February 06, 2015, 18:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudHSMRole

Description: Default policy for the AWS CloudHSM service role.

AWSCloudHSMRole is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudHSMRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC

- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudMapDiscoverInstanceAccess

Description: Provides access to AWS Cloud Map discovery API.

AWSCloudMapDiscoverInstanceAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudMapDiscoverInstanceAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2018, 00:02 UTC
- **Edited time:** September 20, 2023, 21:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudMapFullAccess

Description: Provides full access to all AWS Cloud Map actions.

AWSCloudMapFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudMapFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 23:57 UTC
- **Edited time:** July 29, 2020, 19:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudMapFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudMapReadOnlyAccess

Description: Provides read-only access to all AWS Cloud Map actions.

AWSCloudMapReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudMapReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 23:45 UTC
- **Edited time:** September 20, 2023, 21:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudMapRegisterInstanceAccess

Description: Provides registrant level access to AWS Cloud Map actions.

AWSCloudMapRegisterInstanceAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudMapRegisterInstanceAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2018, 00:04 UTC
- **Edited time:** September 20, 2023, 21:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudShellFullAccess

Description: Grants using AWS CloudShell with all features

AWSCloudShellFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudShellFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 18:07 UTC
- **Edited time:** December 15, 2020, 18:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudTrail_FullAccess

Description: Provides full access to AWS CloudTrail.

AWSCloudTrail_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudTrail_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 08, 2020, 23:41 UTC
- **Edited time:** February 22, 2021, 19:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudTrail_ReadOnlyAccess

Description: Provides read only access to AWS CloudTrail.

AWSCloudTrail_ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCloudTrail_ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 14, 2022, 17:19 UTC
- **Edited time:** June 14, 2022, 17:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Description: This policy is used by the service-linked role named `AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents`. CloudWatch uses this service-linked role to perform AWS System Manager Incident Manager actions when a CloudWatch alarm goes in to ALARM state. This policy grants permission to start incidents on your behalf.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 27, 2021, 13:30 UTC
- **Edited time:** April 27, 2021, 13:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeArtifactAdminAccess

Description: Provides full access to AWS CodeArtifact via the AWS Management Console.

AWSCodeArtifactAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeArtifactAdminAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 16, 2020, 23:53 UTC
- **Edited time:** June 16, 2020, 23:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
} ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeArtifactReadOnlyAccess

Description: Provides read only access to AWS CodeArtifact via the AWS Management Console.

AWSCodeArtifactReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeArtifactReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 25, 2020, 21:23 UTC
- **Edited time:** June 25, 2020, 21:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeBuildAdminAccess

Description: Provides full access to AWS CodeBuild via the AWS Management Console. Also attach AmazonS3ReadOnlyAccess to provide access to download build artifacts, and attach IAMFullAccess to create and manage the service role for CodeBuild.

AWSCodeBuildAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeBuildAdminAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2016, 19:04 UTC
- **Edited time:** May 02, 2024, 01:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeBuildDeveloperAccess

Description: Provides access to AWS CodeBuild via the AWS Management Console, but does not allow CodeBuild project administration. Also attach AmazonS3ReadOnlyAccess to provide access to download build artifacts.

AWSCodeBuildDeveloperAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeBuildDeveloperAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2016, 19:02 UTC
- **Edited time:** May 02, 2024, 01:36 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

Policy version

Policy version: v15 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeBuildReadOnlyAccess

Description: Provides read only access to AWS CodeBuild via the AWS Management Console. Also attach AmazonS3ReadOnlyAccess to provide access to download build artifacts.

AWSCodeBuildReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeBuildReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2016, 19:03 UTC
- **Edited time:** May 02, 2024, 01:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

Policy version

Policy version: v12 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeCommitFullAccess

Description: Provides full access to AWS CodeCommit via the AWS Management Console.

AWSCodeCommitFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeCommitFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:02 UTC
- **Edited time:** July 17, 2023, 21:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeCommitPowerUser

Description: Provides full access to AWS CodeCommit repositories, but does not allow repository deletion.

AWSCodeCommitPowerUser is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeCommitPowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:06 UTC
- **Edited time:** July 17, 2023, 21:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

Policy version

Policy version: v15 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeCommitReadOnly

Description: Provides read only access to AWS CodeCommit via the AWS Management Console.

AWSCodeCommitReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeCommitReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:05 UTC
- **Edited time:** August 18, 2021, 18:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployDeployerAccess

Description: Provides access to register and deploy a revision.

AWSCodeDeployDeployerAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployDeployerAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 19, 2015, 18:18 UTC
- **Edited time:** April 02, 2020, 16:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployFullAccess

Description: Provides full access to CodeDeploy resources.

AWSCodeDeployFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSCodeDeployFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 19, 2015, 18:13 UTC
- **Edited time:** April 02, 2020, 16:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployReadOnlyAccess

Description: Provides read only access to CodeDeploy resources.

AWSCodeDeployReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 19, 2015, 18:21 UTC
- **Edited time:** April 02, 2020, 16:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```

"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" : "*"
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRole

Description: Provides CodeDeploy service access to expand tags and interact with Auto Scaling on your behalf.

AWSCodeDeployRole is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 04, 2015, 18:05 UTC
- **Edited time:** August 16, 2023, 20:38 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRoleForCloudFormation

Description: Provides CodeDeploy service access to invoke Lambda function on your behalf to perform blue/green deployment through CloudFormation.

AWSCodeDeployRoleForCloudFormation is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRoleForCloudFormation to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 19, 2020, 17:12 UTC
- **Edited time:** May 19, 2020, 17:12 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRoleForECS

Description: Provides CodeDeploy service wide access to perform an ECS blue/green deployment on your behalf. Grants full access to support services, such as full access to read all S3 objects, invoke all Lambda functions, publish to all SNS topics within the account and update all ECS services.

AWSCodeDeployRoleForECS is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRoleForECS to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 20:40 UTC
- **Edited time:** September 23, 2019, 22:37 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRoleForECSLimited

Description: Provides CodeDeploy service limited access to perform an ECS blue/green deployment on your behalf.

AWSCodeDeployRoleForECSLimited is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRoleForECSLimited to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 20:42 UTC
- **Edited time:** September 23, 2019, 22:10 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRoleForLambda

Description: Provides CodeDeploy service access to perform a Lambda deployment on your behalf.

AWSCodeDeployRoleForLambda is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRoleForLambda to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 28, 2017, 14:05 UTC
- **Edited time:** December 03, 2019, 19:53 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeDeployRoleForLambdaLimited

Description: Provides CodeDeploy service limited access to perform a Lambda deployment on your behalf.

AWSCodeDeployRoleForLambdaLimited is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeDeployRoleForLambdaLimited to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 17, 2020, 17:14 UTC
- **Edited time:** August 17, 2020, 17:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodePipeline_FullAccess

Description: Provides full access to AWS CodePipeline via the AWS Management Console.

AWSCodePipeline_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodePipeline_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 03, 2020, 22:38 UTC
- **Edited time:** March 14, 2024, 17:06 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodePipeline_ReadOnlyAccess

Description: Provides read only access to AWS CodePipeline via the AWS Management Console.

AWSCodePipeline_ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodePipeline_ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 03, 2020, 22:25 UTC
- **Edited time:** August 03, 2020, 22:25 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodePipelineApproverAccess

Description: Provides access to view and approve manual changes for all pipelines

AWSCodePipelineApproverAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodePipelineApproverAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 28, 2016, 18:59 UTC
- **Edited time:** August 02, 2017, 17:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodePipelineCustomActionAccess

Description: Provides access for custom actions to poll for jobs details (including temporary credentials) and report status updates to AWS CodePipeline.

AWSCodePipelineCustomActionAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodePipelineCustomActionAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:02 UTC
- **Edited time:** July 09, 2015, 17:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeStarFullAccess

Description: Provides full access to AWS CodeStar via the AWS Management Console.

AWSCodeStarFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSCodeStarFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 19, 2017, 16:23 UTC
- **Edited time:** March 28, 2023, 00:06 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCodeStarFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeStarNotificationsServiceRolePolicy

Description: Allows AWS CodeStar Notifications to access Amazon CloudWatch Events on your behalf

AWSCodeStarNotificationsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 05, 2019, 16:10 UTC
- **Edited time:** March 19, 2020, 16:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCodeStarServiceRole

Description: DO NOT USE - AWS CodeStar Service Role Policy which grants administrative privileges in order for CodeStar to manage IAM and other service resources on behalf of the customer.

AWSCodeStarServiceRole is an [AWS managed policy](#).

Using this policy

You can attach `AWSCodeStarServiceRole` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 19, 2017, 15:20 UTC
- **Edited time:** September 20, 2021, 19:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCompromisedKeyQuarantine

Description: Denies access to certain actions, applied by the AWS team in the event that an IAM user's credentials have been compromised or exposed publicly. Do NOT remove this policy. Instead, please follow the instructions specified in the email sent to you regarding this event.

AWSCompromisedKeyQuarantine is an [AWS managed policy](#).

Using this policy

You can attach AWSCompromisedKeyQuarantine to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 11, 2020, 18:04 UTC
- **Edited time:** August 11, 2020, 18:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCompromisedKeyQuarantineV2

Description: Denies access to certain actions, applied by the AWS team in the event that an IAM user's credentials have been compromised or exposed publicly. Do NOT remove this policy. Instead, please follow the instructions specified in the support case created for you regarding this event.

AWSCompromisedKeyQuarantineV2 is an [AWS managed policy](#).

Using this policy

You can attach AWSCompromisedKeyQuarantineV2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 21, 2021, 22:30 UTC
- **Edited time:** March 16, 2023, 00:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigMultiAccountSetupPolicy

Description: Allows Config to call AWS services and deploy config resources across organization

AWSConfigMultiAccountSetupPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 17, 2019, 18:03 UTC
- **Edited time:** February 24, 2023, 01:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigRemediationServiceRolePolicy

Description: Allows AWS Config to remediate noncompliant resources on your behalf.

AWSConfigRemediationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 18, 2019, 21:21 UTC
- **Edited time:** June 18, 2019, 21:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigRoleForOrganizations

Description: Allows AWS Config to call read-only AWS Organizations APIs

AWSConfigRoleForOrganizations is an [AWS managed policy](#).

Using this policy

You can attach AWSConfigRoleForOrganizations to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 19, 2018, 22:53 UTC
- **Edited time:** November 24, 2020, 20:19 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigRulesExecutionRole

Description: Allows an AWS Lambda function to access the AWS Config API and the configuration snapshots that AWS Config delivers periodically to Amazon S3. This access is required by functions that evaluate configuration changes for custom Config rules.

AWSConfigRulesExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSConfigRulesExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 25, 2016, 17:59 UTC
- **Edited time:** May 13, 2019, 21:33 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigServiceRolePolicy

Description: Allows Config to call AWS services and collect resource configurations on your behalf.

AWSConfigServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 30, 2018, 23:31 UTC
- **Edited time:** June 17, 2024, 18:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Policy version

Policy version: v51 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
```

```
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
"emr-containers: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:ListGroupsWithUser",
"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",
"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",
"redshift:DescribeTags",
"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",
"ssm-sap: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/*"
  ]
}
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConfigUserAccess

Description: Provides access to use AWS Config, including searching by tags on resources, and reading all tags. This does not provide permission to configure AWS Config, which requires administrative privileges.

AWSConfigUserAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSConfigUserAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 18, 2015, 19:38 UTC
- **Edited time:** March 18, 2019, 20:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSConnector

Description: Enables broad read/write access to ALL EC2 objects, read/write access to S3 buckets starting with 'import-to-ec2-', and the ability to list all S3 buckets, for the AWS Connector to import VMs on your behalf.

AWSConnector is an [AWS managed policy](#).

Using this policy

You can attach AWSConnector to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 11, 2015, 17:14 UTC
- **Edited time:** September 28, 2015, 19:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSConnector

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSControlTowerAccountServiceRolePolicy

Description: Allows AWS Control Tower to call AWS services that provide automated account configuration and centralized governance on your behalf.

AWSControlTowerAccountServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 05, 2023, 22:04 UTC
- **Edited time:** June 05, 2023, 22:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSControlTowerServiceRolePolicy

Description: Provides access to AWS Resources managed or used by AWS Control Tower

AWSControlTowerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSControlTowerServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 03, 2019, 18:19 UTC
- **Edited time:** April 12, 2023, 19:15 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSCostAndUsageReportAutomationPolicy

Description: Grants permissions to to describe the organization of the account, create S3 buckets for the MAP program and apply tags to it, create a Cost and Usage Report, and describe Cost and Usage Report definitions.

AWSCostAndUsageReportAutomationPolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSCostAndUsageReportAutomationPolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 01, 2021, 21:27 UTC
- **Edited time:** November 01, 2021, 21:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataExchangeFullAccess

Description: Grants full access to AWS Data Exchange and AWS Marketplace actions using the AWS Management Console and SDK. It also provides select access to related services needed to take full advantage of AWS Data Exchange.

AWSDataExchangeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataExchangeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2019, 19:27 UTC
- **Edited time:** June 24, 2024, 19:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
  },
  {
    "Sid" : "S3GetActionConditionalTagAndADX",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/AWSDataExchange" : "true"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "S3WriteActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource" : "arn:aws:s3::*aws-data-exchange*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "S3ReadActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
```

```
"Sid" : "AWSMarketplaceProviderActions",
"Effect" : "Allow",
"Action" : [
  "aws-marketplace:DescribeEntity",
  "aws-marketplace:ListEntities",
  "aws-marketplace:StartChangeSet",
  "aws-marketplace:ListChangeSets",
  "aws-marketplace:DescribeChangeSet",
  "aws-marketplace:CancelChangeSet",
  "aws-marketplace:GetAgreementApprovalRequest",
  "aws-marketplace:ListAgreementApprovalRequests",
  "aws-marketplace:AcceptAgreementApprovalRequest",
  "aws-marketplace:RejectAgreementApprovalRequest",
  "aws-marketplace:UpdateAgreementApprovalRequest",
  "aws-marketplace:SearchAgreements",
  "aws-marketplace:GetAgreementTerms",
  "aws-marketplace:TagResource",
  "aws-marketplace:UntagResource",
  "aws-marketplace:ListTagsForResource"
],
"Resource" : "*"
},
{
  "Sid" : "AWSMarketplaceSubscriberActions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:Subscribe",
    "aws-marketplace:Unsubscribe",
    "aws-marketplace:ViewSubscriptions",
    "aws-marketplace:GetAgreementRequest",
    "aws-marketplace:ListAgreementRequests",
    "aws-marketplace:CancelAgreementRequest",
    "aws-marketplace:ListPrivateListings",
    "aws-marketplace:DescribeAgreement"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KMSActions",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys"
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RedshiftConditionalActions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:AuthorizeDataShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "redshift:ConsumerIdentifier" : "ADX"
      }
    }
  },
  {
    "Sid" : "RedshiftActions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeDataSharesForProducer",
      "redshift:DescribeDataShares"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "APIGatewayActions",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataExchangeProviderFullAccess

Description: Grants data provider access to AWS Data Exchange and AWS Marketplace actions using the AWS Management Console and SDK. It also provides select access to related services needed to take full advantage of AWS Data Exchange.

AWSDataExchangeProviderFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataExchangeProviderFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2019, 19:27 UTC
- **Edited time:** March 15, 2022, 16:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataExchangeReadOnly

Description: Grants read-only access to AWS Data Exchange and AWS Marketplace actions using the AWS Management Console and SDK.

AWSDataExchangeReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSDataExchangeReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2019, 19:27 UTC
- **Edited time:** May 10, 2021, 21:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataExchangeSubscriberFullAccess

Description: Grants data subscriber access to AWS Data Exchange and AWS Marketplace actions using the AWS Management Console and SDK. It also provides select access to related services needed to take full advantage of AWS Data Exchange.

AWSDataExchangeSubscriberFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataExchangeSubscriberFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2019, 19:27 UTC
- **Edited time:** May 21, 2024, 17:36 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataLifecycleManagerServiceRole

Description: Provides appropriate permissions to AWS Data Lifecycle Manager to take actions on AWS resources

AWSDataLifecycleManagerServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AWSDataLifecycleManagerServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** July 06, 2018, 19:34 UTC
- **Edited time:** September 19, 2022, 17:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

Description: Provides appropriate permissions to AWS Data Lifecycle Manager to take actions on AWS resources for AMI Management

AWSDataLifecycleManagerServiceRoleForAMIManagement is an [AWS managed policy](#).

Using this policy

You can attach AWSDataLifecycleManagerServiceRoleForAMIManagement to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 21, 2020, 19:39 UTC
- **Edited time:** August 19, 2021, 17:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataLifecycleManagerSSMFullAccess

Description: Provides Amazon Data Lifecycle Manager permission to perform the Systems Manager actions required to run pre and post scripts on all Amazon EC2 instances.

AWSDataLifecycleManagerSSMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataLifecycleManagerSSMFullAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 31, 2023, 20:29 UTC
- **Edited time:** November 16, 2023, 22:31 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDatapipeline_FullAccess

Description: Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole access for default Roles.

AWSDatapipeline_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDatapipeline_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** January 19, 2017, 23:14 UTC
- **Edited time:** August 17, 2017, 18:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDatapipeline_PowerUser

Description: Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole access for default Roles.

AWSDatapipeline_PowerUser is an [AWS managed policy](#).

Using this policy

You can attach AWSDatapipeline_PowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 19, 2017, 23:16 UTC
- **Edited time:** August 17, 2017, 18:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDatapipeline_PowerUser

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataSyncDiscoveryServiceRolePolicy

Description: Allows DataSync Discovery to integrate with other AWS services on your behalf.

AWSDataSyncDiscoveryServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 20, 2023, 22:19 UTC
- **Edited time:** March 20, 2023, 22:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```



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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataSyncFullAccess

Description: Provides full access to AWS DataSync and minimal access to its dependencies

AWSDataSyncFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataSyncFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 18, 2019, 19:40 UTC
- **Edited time:** February 16, 2024, 17:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDataSyncFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDataSyncReadOnlyAccess

Description: Provides read-only access to AWS DataSync

AWSDataSyncReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDataSyncReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 18, 2019, 19:18 UTC
- **Edited time:** June 30, 2020, 17:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-FleetWorker

Description: Provides AWS Deadline Cloud workers with access to run tasks on a farm.

AWSDeadlineCloud-FleetWorker is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-FleetWorker to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 17:21 UTC
- **Edited time:** April 01, 2024, 17:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-UserAccessFarms

Description: Provides user workstation access to AWS Deadline Cloud farms with limited Read-Only permissions to call other necessary services. Attach this policy to the user role associated with your studio.

AWSDeadlineCloud-UserAccessFarms is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-UserAccessFarms to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 16:54 UTC
- **Edited time:** April 01, 2024, 16:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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}"
    }
  }
}

```

```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-UserAccessFleets

Description: Provides user workstation access to AWS Deadline Cloud fleets with limited Read-Only permissions to call other necessary services. Attach this policy to the user role associated with your studio.

AWSDeadlineCloud-UserAccessFleets is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-UserAccessFleets to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 17:01 UTC
- **Edited time:** April 01, 2024, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-UserAccessJobs

Description: Provides user workstation access to AWS Deadline Cloud jobs with limited Read-Only permissions to call other necessary services. Attach this policy to the user role associated with your studio.

AWSDeadlineCloud-UserAccessJobs is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-UserAccessJobs to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 17:05 UTC
- **Edited time:** April 01, 2024, 17:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-UserAccessQueues

Description: Provides user workstation access to AWS Deadline Cloud queues with limited Read-Only permissions to call other necessary services. Attach this policy to the user role associated with your studio.

AWSDeadlineCloud-UserAccessQueues is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-UserAccessQueues to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 17:10 UTC
- **Edited time:** April 01, 2024, 17:10 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeadlineCloud-WorkerHost

Description: Provides access for AWS Deadline Cloud worker hosts to join a fleet in a farm.

AWSDeadlineCloud-WorkerHost is an [AWS managed policy](#).

Using this policy

You can attach AWSDeadlineCloud-WorkerHost to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2024, 17:28 UTC
- **Edited time:** April 01, 2024, 17:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Sid" : "JoinFleetPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:CreateWorker",
    "deadline:AssumeFleetRoleForWorker"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepLensLambdaFunctionAccessPolicy

Description: This policy specifies permissions required by DeepLens Administrative lambda functions that run on a DeepLens device

AWSDeepLensLambdaFunctionAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepLensLambdaFunctionAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 15:47 UTC

- **Edited time:** June 11, 2019, 23:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepLensServiceRolePolicy

Description: Grants AWS DeepLens access to AWS services, resources and roles needed by DeepLens and its dependencies including IoT, S3, GreenGrass and AWS Lambda.

AWSDeepLensServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepLensServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 29, 2017, 15:46 UTC
- **Edited time:** September 25, 2019, 19:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerAccountAdminAccess

Description: DeepRacer admin access to all actions including toggling between multiuser and single user mode.

AWSDeepRacerAccountAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepRacerAccountAdminAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** October 28, 2021, 01:27 UTC
- **Edited time:** October 28, 2021, 01:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerCloudFormationAccessPolicy

Description: Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

AWSDeepRacerCloudFormationAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepRacerCloudFormationAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 28, 2019, 21:59 UTC
- **Edited time:** June 14, 2019, 17:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerDefaultMultiUserAccess

Description: DeepRacer MultiUser Default user access to use deepracer in multi-user mode

AWSDeepRacerDefaultMultiUserAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSDeepRacerDefaultMultiUserAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 28, 2021, 01:27 UTC
- **Edited time:** October 28, 2021, 01:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer>Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer>Delete*",
        "deepracer:Stop*",

```

```
    "deepracer:Import*",
    "deepracer:Tag*",
    "deepracer:Untag*"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "Null" : {
      "deepracer:UserToken" : "false"
    },
    "Bool" : {
      "deepracer:MultiUser" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "deepracer:GetAccountConfig",
    "deepracer:GetTrack",
    "deepracer:ListTracks",
    "deepracer:TestRewardFunction"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "deepracer:Admin*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerFullAccess

Description: Provides full access to AWS DeepRacer. Also provides select access to related services (e.g., S3).

AWSDeepRacerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepRacerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 05, 2020, 22:03 UTC
- **Edited time:** October 05, 2020, 22:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerRoboMakerAccessPolicy

Description: Allows RoboMaker to create required resources and call AWS services on your behalf.

AWSDeepRacerRoboMakerAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepRacerRoboMakerAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 28, 2019, 21:59 UTC
- **Edited time:** February 28, 2019, 21:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeepRacerServiceRolePolicy

Description: Allows DeepRacer to create required resources and call AWS services on your behalf.

AWSDeepRacerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDeepRacerServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 28, 2019, 21:58 UTC
- **Edited time:** June 12, 2019, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDenyAll

Description: Deny all access.

AWSDenyAll is an [AWS managed policy](#).

Using this policy

You can attach AWSDenyAll to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 01, 2019, 22:36 UTC
- **Edited time:** December 18, 2023, 16:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDenyAll

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeviceFarmFullAccess

Description: Provides full access to all AWS Device Farm operations.

AWSDeviceFarmFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDeviceFarmFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 13, 2015, 16:37 UTC
- **Edited time:** July 13, 2015, 16:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeviceFarmServiceRolePolicy

Description: Grant permissions to AWS Device Farm to call EC2 Network APIs on your behalf.

AWSDeviceFarmServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 20, 2022, 21:02 UTC
- **Edited time:** September 20, 2022, 21:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDeviceFarmTestGridServiceRolePolicy

Description: Grant permissions to AWS Device Farm to call EC2 APIs on your behalf.

AWSDeviceFarmTestGridServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 26, 2021, 22:01 UTC
- **Edited time:** May 26, 2021, 22:01 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDirectConnectFullAccess

Description: Provides full access to AWS Direct Connect via the AWS Management Console.

AWSDirectConnectFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDirectConnectFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** April 30, 2019, 15:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDirectConnectFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    "Action" : [
      "directconnect:*",
      "ec2:DescribeVpnGateways",
      "ec2:DescribeTransitGateways"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDirectConnectReadOnlyAccess

Description: Provides read only access to AWS Direct Connect via the AWS Management Console.

AWSDirectConnectReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDirectConnectReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** May 18, 2020, 18:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDirectConnectServiceRolePolicy

Description: Provides AWS Direct Connect permission to create and manage AWS resources on your behalf.

AWSDirectConnectServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 14, 2021, 18:35 UTC
- **Edited time:** January 14, 2021, 18:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDirectoryServiceFullAccess

Description: Provides full access to AWS Directory Service.

AWSDirectoryServiceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSDirectoryServiceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** April 02, 2024, 20:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDirectoryServiceReadOnlyAccess

Description: Provides read only access to AWS Directory Service.

AWSDirectoryServiceReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSDirectoryServiceReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** September 25, 2018, 21:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDiscoveryContinuousExportFirehosePolicy

Description: Provides write access to AWS resources required for AWS Discovery Continuous Export

AWSDiscoveryContinuousExportFirehosePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSDiscoveryContinuousExportFirehosePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 09, 2018, 18:29 UTC
- **Edited time:** June 08, 2021, 17:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDMSFleetAdvisorServiceRolePolicy

Description: Allows DMS Fleet Advisor to manage CloudWatch metrics on your behalf.

AWSDMSFleetAdvisorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 06, 2023, 09:10 UTC
- **Edited time:** March 06, 2023, 09:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSDMSServerlessServiceRolePolicy

Description: Grants AWS DMS Serverless permissions to create and manage DMS resources in your account on your behalf

AWSDMSServerlessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 18, 2023, 20:28 UTC
- **Edited time:** May 18, 2023, 20:28 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEC2CapacityReservationFleetRolePolicy

Description: Allows EC2 CapacityReservation Fleet service to manage Capacity Reservations

AWSEC2CapacityReservationFleetRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 29, 2021, 14:43 UTC
- **Edited time:** September 29, 2021, 14:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
    }
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEC2FleetServiceRolePolicy

Description: Allows EC2 Fleet to launch and manage instances.

AWSEC2FleetServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 21, 2018, 00:08 UTC
- **Edited time:** May 04, 2020, 20:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEC2SpotFleetServiceRolePolicy

Description: Allows EC2 Spot Fleet to launch and manage spot fleet instances

AWSEC2SpotFleetServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 23, 2017, 19:13 UTC
- **Edited time:** March 16, 2020, 19:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEC2SpotServiceRolePolicy

Description: Allows EC2 Spot to launch and manage spot instances

AWSEC2SpotServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 18, 2017, 18:51 UTC
- **Edited time:** December 12, 2018, 00:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEC2VssSnapshotPolicy

Description: This policy is attached to the IAM role that's attached to your Amazon EC2 Windows Instances to enable the Amazon EC2 VSS solution to create and add tags to Amazon Machine Images (AMI) and EBS Snapshots.

AWSEC2VssSnapshotPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSEC2VssSnapshotPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 27, 2024, 16:32 UTC
- **Edited time:** March 27, 2024, 16:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSECRPullThroughCache_ServiceRolePolicy

Description: Enables access to AWS services and resources used or managed by AWS ECR pull through cache

AWSECRPullThroughCache_ServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2021, 21:51 UTC
- **Edited time:** November 13, 2023, 15:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

Description: Provide the instance in your custom platform builder environment permission to launch EC2 instance, create EBS snapshot and AMI, stream logs to Amazon CloudWatch Logs, and store artifacts in Amazon S3.

AWSElasticBeanstalkCustomPlatformforEC2Role is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkCustomPlatformforEC2Role to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 21, 2017, 22:50 UTC
- **Edited time:** February 21, 2017, 22:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkEnhancedHealth

Description: AWS Elastic Beanstalk Service policy for Health Monitoring system

AWSElasticBeanstalkEnhancedHealth is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkEnhancedHealth to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 08, 2016, 23:17 UTC
- **Edited time:** April 09, 2018, 22:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS Elastic Beanstalk Maintenance

Description: AWS Elastic Beanstalk Service Role policy that grants limited permissions to update your resources on your behalf for maintenance purposes.

AWS Elastic Beanstalk Maintenance is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 11, 2019, 23:22 UTC
- **Edited time:** April 29, 2024, 21:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Description: This policy is for the AWS Elastic Beanstalk service role used to perform managed updates of Elastic Beanstalk environments. This policy should not be attached to other users or roles. The policy grants broad permissions to create and manage resources across a number of AWS services including AutoScaling, EC2, ECS, Elastic Load Balancing and CloudFormation. This policy also allows passing of any IAM role usable with those services.

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 03, 2021, 22:18 UTC
- **Edited time:** March 23, 2023, 23:15 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Description: AWS Elastic Beanstalk Service Role policy that grants limited permissions to managed updates.

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 21, 2019, 22:35 UTC
- **Edited time:** April 29, 2024, 23:11 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    }  
  ]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkMulticontainerDocker

Description: Provide the instances in your multicontainer Docker environment access to use the Amazon EC2 Container Service to manage container deployment tasks.

AWSElasticBeanstalkMulticontainerDocker is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkMulticontainerDocker to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 08, 2016, 23:15 UTC
- **Edited time:** March 23, 2023, 22:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkReadOnly

Description: Grants read-only permissions. Explicitly allows operators to gain direct access to retrieve information about resources related to AWS Elastic Beanstalk applications.

AWSElasticBeanstalkReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 22, 2021, 19:02 UTC
- **Edited time:** January 22, 2021, 19:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleCore

Description: AWSElasticBeanstalkRoleCore (Elastic Beanstalk operations role) Allows core operation of a web service environment.

AWSElasticBeanstalkRoleCore is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleCore to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:48 UTC
- **Edited time:** April 30, 2024, 00:01 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Sid" : "TerminateInstances",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
      }
    }
  },
  {
    "Sid" : "EC2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ReleaseAddress",
      "ec2:AllocateAddress",
      "ec2:DisassociateAddress",
      "ec2:AssociateAddress",
      "ec2:CreateTags",
      "ec2>DeleteTags",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:AuthorizeSecurityGroup*",
      "ec2:RevokeSecurityGroup*",
      "ec2:CreateLaunchTemplate*",
      "ec2>DeleteLaunchTemplate*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LTRunInstances",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  }
]
```

```

    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ]
    },

```



```
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3Obj",
    "Effect" : "Allow",
    "Action" : [
      "s3:Delete*",
      "s3:Get*",
      "s3:Put*"
    ],
    "Resource" : [
      "arn:aws:s3:::elasticbeanstalk-*/**",
      "arn:aws:s3:::elasticbeanstalk-env-resources-*/**"
    ]
  },
  {
    "Sid" : "S3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucket*",
      "s3:ListBucket",
      "s3:PutBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
  },
  {
    "Sid" : "CFN",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:GetTemplate",
      "cloudformation:ListStackResources",
      "cloudformation:UpdateStack",
      "cloudformation:ContinueUpdateRollback",
      "cloudformation:CancelUpdateStack",
      "cloudformation:TagResource",
      "cloudformation:UntagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
```

```

},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
},
{
  "Sid" : "ELB",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:Create*",
    "elasticloadbalancing>Delete*",
    "elasticloadbalancing:Modify*",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:DeRegisterTargets",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:*Tags",
    "elasticloadbalancing:ConfigureHealthCheck",
    "elasticloadbalancing:SetRulePriorities",
    "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/**",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/**",
    "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/**/**"
  ]
},
{
  "Sid" : "ListAPIs",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*",
    "cloudformation:Describe*",
    "logs:Describe*",

```

```
    "ec2:Describe*",
    "ecs:Describe*",
    "ecs:List*",
    "elasticloadbalancing:Describe*",
    "rds:Describe*",
    "sns:List*",
    "iam:List*",
    "acm:Describe*",
    "acm:List*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPassRole",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "elasticbeanstalk.amazonaws.com",
        "ec2.amazonaws.com",
        "autoscaling.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "ecs.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleCWL

Description: (Elastic Beanstalk operations role) Allows an environment to manage Amazon CloudWatch Logs log groups.

AWSElasticBeanstalkRoleCWL is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleCWL to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:49 UTC
- **Edited time:** June 05, 2020, 21:49 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ]
    }
  ],
}
```

```
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleECS

Description: (Elastic Beanstalk operations role) Allows a multicontainer Docker environment to manage Amazon ECS clusters.

AWSElasticBeanstalkRoleECS is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleECS to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:47 UTC
- **Edited time:** March 23, 2023, 22:43 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleRDS

Description: (Elastic Beanstalk operations role) Allows an environment to integrate an Amazon RDS instance.

AWSElasticBeanstalkRoleRDS is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleRDS to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:46 UTC
- **Edited time:** June 05, 2020, 21:46 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleSNS

Description: (Elastic Beanstalk operations role) Allows an environment to enable Amazon SNS topic integration.

AWSElasticBeanstalkRoleSNS is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleSNS to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:46 UTC
- **Edited time:** June 05, 2020, 21:46 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkRoleWorkerTier

Description: (Elastic Beanstalk operations role) Allows a worker environment tier to create an Amazon DynamoDB table and an Amazon SQS queue.

AWSElasticBeanstalkRoleWorkerTier is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkRoleWorkerTier to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2020, 21:43 UTC
- **Edited time:** June 05, 2020, 21:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS Elastic Beanstalk Service

Description: This policy is on a deprecation path. See documentation for guidance: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Elastic Beanstalk Service role policy which grants permissions to create & manage resources (i.e.: AutoScaling, EC2, S3, CloudFormation, ELB, etc.) on your behalf.

AWS Elastic Beanstalk Service is an [AWS managed policy](#).

Using this policy

You can attach `AWSElasticBeanstalkService` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 11, 2016, 20:27 UTC
- **Edited time:** May 10, 2023, 19:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Policy version

Policy version: v17 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkServiceRolePolicy

Description: AWS Elastic Beanstalk Service Linked Role policy which grants permissions to create & manage resources (i.e.: AutoScaling, EC2, S3, CloudFormation, ELB, etc.) on your behalf.

AWSElasticBeanstalkServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 13, 2017, 23:46 UTC
- **Edited time:** June 06, 2019, 21:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkWebTier

Description: Provide the instances in your web server environment access to upload log files to Amazon S3.

AWSElasticBeanstalkWebTier is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkWebTier to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 08, 2016, 23:08 UTC
- **Edited time:** September 09, 2020, 19:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticBeanstalkWorkerTier

Description: Provide the instances in your worker environment access to upload log files to Amazon S3, to use Amazon SQS to monitor your application's job queue, to use Amazon DynamoDB to perform leader election, and to Amazon CloudWatch to publish metrics for health monitoring.

AWSElasticBeanstalkWorkerTier is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticBeanstalkWorkerTier to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 08, 2016, 23:12 UTC
- **Edited time:** September 09, 2020, 19:53 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

Description: This policy allows installing the AWS Replication Agent, which is used with AWS Elastic Disaster Recovery (DRS) to recover external servers to AWS. Attach this policy to your IAM users or roles whose credentials you provide during the installation step of the AWS Replication Agent.

AWSElasticDisasterRecoveryAgentInstallationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryAgentInstallationPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2021, 10:37 UTC

- **Edited time:** November 27, 2023, 12:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryAgentPolicy

Description: This policy allows using the AWS Replication Agent, which is used with AWS Elastic Disaster Recovery (DRS) to recover source servers to AWS. We do not recommend that you attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryAgentPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryAgentPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 17, 2021, 10:32 UTC
- **Edited time:** November 27, 2023, 13:44 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS Elastic Disaster Recovery Console Full Access

Description: This policy provides full access to all public APIs of AWS Elastic Disaster Recovery (DRS), as well as permissions to read KMS key, License Manager, Resource Groups, Elastic Load Balancing, IAM, and EC2 information. Attach this policy to your IAM users or roles.

AWS Elastic Disaster Recovery Console Full Access is an [AWS managed policy](#).

Using this policy

You can attach `AWSElasticDisasterRecoveryConsoleFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2021, 10:46 UTC
- **Edited time:** October 16, 2023, 12:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Description: This policy provides full access to all public APIs of AWS Elastic Disaster Recovery (AWS DRS), as well as all public APIs in other AWS services used by AWS DRS Console. Attach this policy to your users or roles.

AWSElasticDisasterRecoveryConsoleFullAccess_v2 is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryConsoleFullAccess_v2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2023, 13:35 UTC
- **Edited time:** May 19, 2024, 07:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```



```
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess4",
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess5",
  "Effect" : "Allow",
  "Action" : "resource-groups:ListGroups",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess6",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess7",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess8",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
```

```

    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions",
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "ConsoleFullAccess11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess15",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
```

```
"Sid" : "ConsoleFullAccess16",
"Effect" : "Allow",
"Action" : "ec2:CreateSecurityGroup",
"Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "ConsoleFullAccess17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess19",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess20",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess21",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume",
    "ec2:StartInstances",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Sid" : "ConsoleFullAccess22",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess23",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess24",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  },
}
```

```
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Sid" : "ConsoleFullAccess25",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess26",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      }
    }
  },
}
```



```
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Sid" : "ConsoleFullAccess27",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess28",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess29",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess30",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation",
      "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"
      }
    }
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryConversionServerPolicy

Description: This policy is attached to the AWS Elastic Disaster Recovery Conversion server's instance role. This policy allows Elastic Disaster Recovery (DRS) Conversion Servers, which are EC2 instances launched by Elastic Disaster Recovery, to communicate with the DRS service. An IAM role with this policy is attached (as an EC2 Instance Profile) by DRS to the DRS Conversion Servers, which are automatically launched and terminated by DRS, when needed. We do not recommend that you attach this policy to your IAM users or roles. DRS Conversion Servers are used by Elastic Disaster Recovery when users choose to recover source servers using the DRS console, CLI, or API.

AWSElasticDisasterRecoveryConversionServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryConversionServerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 17, 2021, 13:42 UTC
- **Edited time:** November 27, 2023, 13:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Description: This policy allows AWS Elastic Disaster Recovery (DRS) to support cross-account replication and cross-account failback.

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryCrossAccountReplicationPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 14, 2023, 07:16 UTC
- **Edited time:** January 17, 2024, 13:19 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

Description: This policy allows installing and using the AWS Replication Agent, which is used by AWS Elastic Disaster Recovery (DRS) to recover source servers that run on EC2 (cross-region or cross-AZ). An IAM role with this policy should be attached (as an EC2 Instance Profile) to the EC2 Instances.

AWSElasticDisasterRecoveryEc2InstancePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryEc2InstancePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 26, 2022, 12:30 UTC
- **Edited time:** November 27, 2023, 13:39 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
}

```

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Description: You can attach the AWSElasticDisasterRecoveryFailbackInstallationPolicy policy to your IAM identities. This policy allows installing the Elastic Disaster Recovery Failback Client, which is used to failback Recovery Instances back to your original source infrastructure. Attach this policy to your IAM users or roles whose credentials you provide when running the Elastic Disaster Recovery Failback Client.

AWSElasticDisasterRecoveryFailbackInstallationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryFailbackInstallationPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2021, 11:02 UTC
- **Edited time:** November 27, 2023, 13:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryFailbackPolicy

Description: This policy allows using the Elastic Disaster Recovery Failback Client, which is used to failback Recovery Instances back to your original source infrastructure. We do not recommend that you attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryFailbackPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryFailbackPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 17, 2021, 10:41 UTC
- **Edited time:** November 27, 2023, 12:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

Description: This policy allows you to use Amazon SSM and additional services required permissions to run post-launch actions in AWS Elastic Disaster Recovery (AWS DRS). Attach this policy to your IAM roles or users.

AWSElasticDisasterRecoveryLaunchActionsPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryLaunchActionsPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 13, 2023, 07:38 UTC
- **Edited time:** May 19, 2024, 07:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
            }
        }
    }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Description: This policy allows AWS Elastic Disaster Recovery (DRS) to support network replication.

AWSElasticDisasterRecoveryNetworkReplicationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryNetworkReplicationPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 11, 2023, 12:36 UTC
- **Edited time:** January 02, 2024, 13:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryReadOnlyAccess

Description: You can attach the AWSElasticDisasterRecoveryReadOnlyAccess policy to your IAM identities. This policy provides permissions to all read-only public APIs of Elastic Disaster Recovery (DRS), as well as some read-only APIs of other AWS services that are required in order to make full read-only use of the DRS console. Attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSElasticDisasterRecoveryReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2021, 10:50 UTC
- **Edited time:** November 27, 2023, 13:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Description: This policy is attached to the instance role of Elastic Disaster Recovery's Recovery Instance. This policy allows the Elastic Disaster Recovery (DRS) Recovery Instance, which are EC2 instances launched by Elastic Disaster Recovery - to communicate with the DRS service, and to be able to failback to their original source infrastructure. An IAM role with this policy is attached (as an EC2 Instance Profile) by Elastic Disaster Recovery to the DRS Recovery Instances. We do not recommend that you attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryRecoveryInstancePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryRecoveryInstancePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 17, 2021, 10:20 UTC
- **Edited time:** November 27, 2023, 13:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

Description: This policy is attached to the Elastic Disaster Recovery Replication server's instance role. This policy allows the Elastic Disaster Recovery (DRS) Replication Servers, which are EC2 instances launched by Elastic Disaster Recovery - to communicate with the DRS service, and to create EBS snapshots in your AWS account. An IAM role with this policy is attached (as an EC2 Instance Profile) by Elastic Disaster Recovery to the DRS Replication Servers which are automatically launched and terminated by DRS, as needed. DRS Replication Servers are used to facilitate data replication from your external servers to AWS, as part of the recovery process managed by DRS. We do not recommend that you attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryReplicationServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryReplicationServerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 17, 2021, 13:34 UTC
- **Edited time:** November 27, 2023, 13:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryServiceRolePolicy

Description: This policy allows Elastic Disaster Recovery to manage AWS resources on your behalf.

AWSElasticDisasterRecoveryServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 17, 2021, 10:56 UTC
- **Edited time:** January 17, 2024, 13:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

```
},
{
  "Sid" : "DRSServiceRolePolicy5",
  "Effect" : "Allow",
  "Action" : "kms:ListRetirableGrants",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumeAttribute",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeVpcs",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeManagedPrefixLists",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetManagedPrefixListAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage"
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSServiceRolePolicy8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeregisterImage"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
}
```

```
  },
  {
    "Sid" : "DRSServiceRolePolicy11",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVolume",
      "ec2:ModifyVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy12",
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy13",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
```

```
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
}
},
{
  "Sid" : "DRSServiceRolePolicy14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy15",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy16",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "DRSServiceRolePolicy17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
}
```

```
"Resource" : "arn:aws:ec2:*:*:launch-template/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
},
{
  "Sid" : "DRSServiceRolePolicy18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy19",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy20",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy21",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy22",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*"
},
{
  "Sid" : "DRSServiceRolePolicy23",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy24",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
```



```

        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Sid" : "DRSServiceRolePolicy25",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam:*:*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam:*:*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "ec2.amazonaws.com"
        }
    }
},
{
    "Sid" : "DRSServiceRolePolicy26",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : [
                "CreateLaunchTemplate",
                "CreateSecurityGroup",
                "CreateVolume",
                "CreateSnapshot",
            ]
        }
    }
}

```

```
        "RunInstances"
      ]
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy27",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy28",
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

Description: This policy allows read-only access to AWS Elastic Disaster Recovery (DRS) resources such as source servers and jobs. It also allows creating a converted snapshot and sharing that EBS snapshot with a specific account.

AWSElasticDisasterRecoveryStagingAccountPolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSElasticDisasterRecoveryStagingAccountPolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 26, 2022, 09:49 UTC
- **Edited time:** November 27, 2023, 13:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Description: This policy is used by AWS Elastic Disaster Recovery (DRS) to recover source servers into a separate target account and to allow failing back. We do not recommend that you attach this policy to your IAM users or roles.

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 is an [AWS managed policy](#).

Using this policy

You can attach AWSElasticDisasterRecoveryStagingAccountPolicy_v2 to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 05, 2023, 12:11 UTC
- **Edited time:** November 27, 2023, 13:32 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

Description: Service Linked Role Policy for AWS Elastic Load Balancing Control Plane - Classic

AWSElasticLoadBalancingClassicServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 19, 2017, 22:36 UTC
- **Edited time:** October 07, 2019, 23:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS ElasticLoadBalancingServiceRolePolicy

Description: Service Linked Role Policy for AWS Elastic Load Balancing Control Plane

AWS ElasticLoadBalancingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 19, 2017, 22:19 UTC
- **Edited time:** August 26, 2021, 19:01 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaConvertFullAccess

Description: Provides full access to AWS Elemental MediaConvert via the AWS Management Console and SDK.

AWSElementalMediaConvertFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaConvertFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 25, 2018, 19:25 UTC
- **Edited time:** June 10, 2019, 22:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaConvertReadOnly

Description: Provides read only access to AWS Elemental MediaConvert via the AWS Management Console and SDK.

AWSElementalMediaConvertReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaConvertReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 25, 2018, 19:25 UTC
- **Edited time:** June 10, 2019, 22:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ]
    }
  ]
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaLiveFullAccess

Description: Provides full access to AWS Elemental MediaLive resources

AWSElementalMediaLiveFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaLiveFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 08, 2020, 17:07 UTC
- **Edited time:** July 08, 2020, 17:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaLiveReadOnly

Description: Provides read only access to AWS Elemental MediaLive resources

AWSElementalMediaLiveReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaLiveReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 08, 2020, 16:38 UTC
- **Edited time:** July 08, 2020, 16:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaPackageFullAccess

Description: Provides full access to AWS Elemental MediaPackage resources

AWSElementalMediaPackageFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaPackageFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 29, 2017, 23:39 UTC
- **Edited time:** December 29, 2017, 23:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaPackageReadOnly

Description: Provides read only access to AWS Elemental MediaPackage resources

AWSElementalMediaPackageReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaPackageReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 30, 2017, 00:04 UTC
- **Edited time:** December 30, 2017, 00:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaPackageV2FullAccess

Description: Provides full access to AWS Elemental MediaPackageV2 resources.

AWSElementalMediaPackageV2FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaPackageV2FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 25, 2023, 20:29 UTC
- **Edited time:** July 25, 2023, 20:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaPackageV2ReadOnly

Description: Provides read-only access to AWS Elemental MediaPackageV2 resources.

AWSElementalMediaPackageV2ReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaPackageV2ReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 25, 2023, 20:31 UTC
- **Edited time:** July 25, 2023, 20:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : {
  "Effect" : "Allow",
  "Action" : [
    "mediapackagev2:List*",
    "mediapackagev2:Get*"
  ],
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaStoreFullAccess

Description: Provides full read and write access to all MediaStore APIs

AWSElementalMediaStoreFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaStoreFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 05, 2018, 23:15 UTC
- **Edited time:** March 05, 2018, 23:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaStoreReadOnly

Description: Provides read-only permissions for MediaStore APIs

AWSElementalMediaStoreReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaStoreReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 08, 2018, 19:48 UTC
- **Edited time:** March 08, 2018, 19:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaTailorFullAccess

Description: Provides full access to AWS Elemental MediaTailor resources

AWSElementalMediaTailorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaTailorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 23, 2021, 00:04 UTC
- **Edited time:** November 23, 2021, 00:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSElementalMediaTailorReadOnly

Description: Provides read only access to AWS Elemental MediaTailor resources

AWSElementalMediaTailorReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSElementalMediaTailorReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 23, 2021, 00:05 UTC
- **Edited time:** November 23, 2021, 00:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```



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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEnhancedClassicNetworkingMangementPolicy

Description: Policy to enable enhanced classic networking management feature.

AWSEnhancedClassicNetworkingMangementPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 20, 2017, 17:29 UTC
- **Edited time:** September 20, 2017, 17:29 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEntityResolutionConsoleFullAccess

Description: Provides console full access to AWS Entity Resolution and related services.

AWSEntityResolutionConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSEntityResolutionConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 17, 2023, 17:54 UTC
- **Edited time:** October 16, 2023, 18:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSEntityResolutionConsoleReadOnlyAccess

Description: Provides read-only access to AWS Entity Resolution via the AWS Management Console.

AWSEntityResolutionConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSEntityResolutionConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 17, 2023, 18:18 UTC
- **Edited time:** August 17, 2023, 18:18 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorEC2Access

Description: This policy grants the Fault Injection Simulator Service permission in EC2 and other required services to perform FIS actions.

AWSFaultInjectionSimulatorEC2Access is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorEC2Access to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** October 26, 2022, 20:39 UTC
- **Edited time:** November 27, 2023, 15:08 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorECSAccess

Description: This policy grants the Fault Injection Simulator Service permission in ECS and other required services to perform FIS actions.

AWSFaultInjectionSimulatorECSAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorECSAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 26, 2022, 20:37 UTC
- **Edited time:** January 25, 2024, 16:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorEKSAccess

Description: This policy grants the Fault Injection Simulator Service permission in EKS and other required services to perform FIS actions.

AWSFaultInjectionSimulatorEKSAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorEKSAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 26, 2022, 20:34 UTC

- **Edited time:** November 13, 2023, 16:44 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorNetworkAccess

Description: This policy grants the Fault Injection Simulator Service permission in EC2 networking and other required services to perform FIS actions.

AWSFaultInjectionSimulatorNetworkAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorNetworkAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** October 26, 2022, 20:32 UTC
- **Edited time:** January 25, 2024, 16:07 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorRDSAccess

Description: This policy grants the Fault Injection Simulator Service permission in RDS and other required services to perform FIS actions.

AWSFaultInjectionSimulatorRDSAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorRDSAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 26, 2022, 20:30 UTC
- **Edited time:** November 13, 2023, 16:23 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFaultInjectionSimulatorSSMAccess

Description: This policy grants the Fault Injection Simulator Service permission in SSM and other required services to perform FIS actions.

AWSFaultInjectionSimulatorSSMAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFaultInjectionSimulatorSSMAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 26, 2022, 15:33 UTC
- **Edited time:** June 02, 2023, 22:55 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFinSpaceServiceRolePolicy

Description: Policy to enable access to AWS service and Resources used or managed by Amazon FinSpace

AWSFinSpaceServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 12, 2023, 16:42 UTC
- **Edited time:** December 01, 2023, 21:05 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFMAdminFullAccess

Description: Full access for AWS FM Administrator

AWSFMAdminFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSFMAdminFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2018, 18:06 UTC
- **Edited time:** October 20, 2022, 23:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFMAdminReadOnlyAccess

Description: Read only access for AWS FM Administrator that allows monitoring AWS FM operations

AWSFMAdminReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFMAdminReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2018, 20:07 UTC
- **Edited time:** October 31, 2022, 22:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSFMMemberReadOnlyAccess

Description: Provides read only access to AWS WAF actions for AWS Firewall Manager member accounts

AWSFMMemberReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSFMMemberReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2018, 21:05 UTC
- **Edited time:** May 09, 2018, 21:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSForWordPressPluginPolicy

Description: Managed policy for AWS For Wordpress Plugin

AWSForWordPressPluginPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSForWordPressPluginPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 30, 2019, 00:27 UTC
- **Edited time:** January 20, 2020, 23:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGitSyncServiceRolePolicy

Description: Policy which allows AWS Code Connections to sync content from your git repository

AWSGitSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 16, 2023, 17:05 UTC
- **Edited time:** April 26, 2024, 18:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlobalAcceleratorSLRPolicy

Description: Policy granting permissions to AWS Global Accelerator to manage EC2 Elastic Network Interfaces and Security Groups.

AWSGlobalAcceleratorSLRPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 05, 2019, 19:39 UTC
- **Edited time:** September 12, 2023, 16:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueConsoleFullAccess

Description: Provides full access to AWS Glue via the AWS Management Console

AWSGlueConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 14, 2017, 13:37 UTC
- **Edited time:** July 14, 2023, 14:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueConsoleSageMakerNotebookFullAccess

Description: Provides full access to AWS Glue via the AWS Management Console and access to sagemaker notebook instances.

AWSGlueConsoleSageMakerNotebookFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSGlueConsoleSageMakerNotebookFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 05, 2018, 17:52 UTC
- **Edited time:** July 15, 2021, 15:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AwsGlueDataBrewFullAccessPolicy

Description: Provides full access to AWS Glue DataBrew via the AWS Management Console. Also provides select access to related services (e.g., S3, KMS, Glue).

AwsGlueDataBrewFullAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AwsGlueDataBrewFullAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 11, 2020, 16:51 UTC
- **Edited time:** February 04, 2022, 18:28 UTC
- **ARN:** arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueDataBrewServiceRole

Description: This policy grants permission to glue to perform action on user's glue data catalog, this policy also provides permission to ec2 actions to allow glue to create ENI to connect to resources in the VPC, also allow glue to access registered data in lakeformation and permission to access user's cloudwatch

AWSGlueDataBrewServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueDataBrewServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 04, 2020, 21:26 UTC
- **Edited time:** March 20, 2024, 23:28 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```
{
  "Sid" : "GluePIIPermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:BatchGetCustomEntityTypes",
    "glue:GetCustomEntityType"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "S3PublicDatasetAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::databrew-public-datasets-*"
  ]
},
{
  "Sid" : "EC2NetworkingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteNetworkInterface",
  "Condition" : {
    "StringLike" : {
```

```
        "aws:ResourceTag/aws-glue-service-resource" : "*"
    }
},
"Resource" : [
    "*"
]
},
{
    "Sid" : "EC2GlueTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "aws-glue-service-resource"
            ]
        }
    },
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
    ]
},
{
    "Sid" : "GlueDatabrewLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
    ]
},
{
    "Sid" : "LakeFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "lakeformation:GetDataAccess"
    ]
},
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueSchemaRegistryFullAccess

Description: Provides full access to the AWS Glue Schema Registry Service

AWSGlueSchemaRegistryFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueSchemaRegistryFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 20, 2020, 00:19 UTC
- **Edited time:** November 20, 2020, 00:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
"Effect" : "Allow",
"Action" : [
  "glue:GetTags",
  "glue:TagResource",
  "glue:UntagResource"
],
"Resource" : [
  "arn:aws:glue:*:*:schema/*",
  "arn:aws:glue:*:*:registry/*"
]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueSchemaRegistryReadOnlyAccess

Description: Provides readonly access to the AWS Glue Schema Registry Service

AWSGlueSchemaRegistryReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueSchemaRegistryReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 20, 2020, 00:20 UTC
- **Edited time:** November 20, 2020, 00:20 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueServiceNotebookRole

Description: Policy for AWS Glue service role which allows customer to manage notebook server

AWSGlueServiceNotebookRole is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueServiceNotebookRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 13:37 UTC
- **Edited time:** October 09, 2023, 15:59 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGlueServiceRole

Description: Policy for AWS Glue service role which allows access to related services including EC2, S3, and Cloudwatch Logs

AWSGlueServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AWSGlueServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 13:37 UTC
- **Edited time:** September 11, 2023, 16:39 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AwsGlueSessionUserRestrictedNotebookPolicy

Description: Provides permissions that allows users to create and use only the notebook sessions that are associated with the user. This policy also includes permissions to explicitly allow users to pass a restricted Glue session role.

AwsGlueSessionUserRestrictedNotebookPolicy is an [AWS managed policy](#).

Using this policy

You can attach AwsGlueSessionUserRestrictedNotebookPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 18, 2022, 15:24 UTC
- **Edited time:** November 22, 2023, 01:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

Description: Provides full access to all AWS Glue resources except for sessions. Allows users to create and use only the notebook sessions that are associated with the user. This policy also includes other permissions needed by AWS Glue to manage Glue resources in other AWS services.

AwsGlueSessionUserRestrictedNotebookServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AwsGlueSessionUserRestrictedNotebookServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 18, 2022, 15:27 UTC
- **Edited time:** April 18, 2022, 15:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AwsGlueSessionUserRestrictedPolicy

Description: Provides permissions that allows users to create and use only the interactive sessions that are associated with the user. This policy also includes permissions to explicitly allow users to pass a restricted Glue session role.

AwsGlueSessionUserRestrictedPolicy is an [AWS managed policy](#).

Using this policy

You can attach AwsGlueSessionUserRestrictedPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 14, 2022, 21:31 UTC
- **Edited time:** April 29, 2024, 22:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AwsGlueSessionUserRestrictedServiceRole

Description: Provides full access to all AWS Glue resources except for sessions. Allows users to create and use only the interactive sessions that are associated with the user. This policy also includes other permissions needed by AWS Glue to manage Glue resources in other AWS services

AwsGlueSessionUserRestrictedServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AwsGlueSessionUserRestrictedServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** April 14, 2022, 21:30 UTC
- **Edited time:** April 29, 2024, 22:51 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
```

```
"Effect" : "Allow",
"Action" : [
  "glue:StartCompletion",
  "glue:GetCompletion"
],
"Resource" : [
  "arn:aws:glue:*:*:completion/*"
]
},
{
  "Sid" : "AllowSessionActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/owner" : "${aws:userid}"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Sid" : "AllowStatementActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "AllowListSessionsAction",
    "Effect" : "Allow",
    "Action" : [
      "glue:ListSessions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DenyTagActions",
    "Effect" : "Deny",
    "Action" : [
      "glue:TagResource",
      "glue:UntagResource",
      "tag:TagResources",
      "tag:UntagResources"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    }
  },
  {
    "Sid" : "AllowS3BucketActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  }
}
```

```
]
},
{
  "Sid" : "AllowS3ObjectActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/*aws-glue-*/**"
  ]
},
{
  "Sid" : "AllowS3ObjectCrawlerActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*"
  ]
},
{
  "Sid" : "AllowLogsActions",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*/aws-glue/*"
  ]
},
{
  "Sid" : "AllowTagsActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
}
```

```
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "aws-glue-service-resource"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGrafanaAccountAdministrator

Description: Provides access within Amazon Grafana to create and manage workspaces for the entire organization.

AWSGrafanaAccountAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AWSGrafanaAccountAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 23, 2021, 00:20 UTC
- **Edited time:** February 15, 2022, 22:36 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGrafanaConsoleReadOnlyAccess

Description: Access to read only operations in Amazon Grafana.

AWSGrafanaConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGrafanaConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 23, 2021, 00:10 UTC
- **Edited time:** February 15, 2022, 22:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGrafanaWorkspacePermissionManagement

Description: Provides only the ability to update user and group permissions for AWS Grafana workspaces.

AWSGrafanaWorkspacePermissionManagement is an [AWS managed policy](#).

Using this policy

You can attach AWSGrafanaWorkspacePermissionManagement to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 23, 2021, 00:15 UTC
- **Edited time:** March 15, 2023, 22:17 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGrafanaWorkspacePermissionManagementV2

Description: Provides ability to update IAM Identity Center (IdC) user and group permissions for Amazon Managed Grafana workspaces.

AWSGrafanaWorkspacePermissionManagementV2 is an [AWS managed policy](#).

Using this policy

You can attach AWSGrafanaWorkspacePermissionManagementV2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 05, 2024, 18:39 UTC
- **Edited time:** January 05, 2024, 18:39 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGreengrassFullAccess

Description: This policy gives full access to the AWS Greengrass configuration, management and deployment actions

AWSGreengrassFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGreengrassFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 03, 2017, 00:47 UTC
- **Edited time:** May 03, 2017, 00:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGreengrassFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGreengrassReadOnlyAccess

Description: This policy gives read only access to the AWS Greengrass configuration, management and deployment actions

AWSGreengrassReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSGreengrassReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 30, 2018, 16:01 UTC
- **Edited time:** October 30, 2018, 16:01 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGreengrassResourceAccessRolePolicy

Description: Policy for AWS Greengrass service role which allows access to related services including AWS Lambda and AWS IoT thing shadows.

AWSGreengrassResourceAccessRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSGreengrassResourceAccessRolePolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 14, 2017, 21:17 UTC
- **Edited time:** November 14, 2018, 00:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSGroundStationAgentInstancePolicy

Description: Provides the Dataflow Endpoint Instance permissions to use the AWS Ground Station Agent

AWSGroundStationAgentInstancePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSGroundStationAgentInstancePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 29, 2023, 15:23 UTC
- **Edited time:** March 29, 2023, 15:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSHealth_EventProcessorServiceRolePolicy

Description: Allows AWS Health to enable the Health event processor feature.

AWSHealth_EventProcessorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 13, 2023, 19:24 UTC
- **Edited time:** January 13, 2023, 19:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSHealthFullAccess

Description: Allows full access to the AWS Health Apis and Notifications and the Personal Health Dashboard

AWSHealthFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSHealthFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 06, 2016, 12:30 UTC
- **Edited time:** November 16, 2020, 18:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSHealthImagingFullAccess

Description: Provides full access to AWS Health Imaging service.

AWSHealthImagingFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSHealthImagingFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 25, 2023, 23:39 UTC
- **Edited time:** July 25, 2023, 23:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSHealthImagingReadOnlyAccess

Description: Provides read only access to AWS Health Imaging service.

AWSHealthImagingReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSHealthImagingReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 25, 2023, 23:40 UTC
- **Edited time:** August 01, 2023, 15:18 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIAMIdentityCenterAllowListForIdentityContext

Description: Provides the list of actions that are allowed for roles assumed with the IAM Identity Center identity context. AWS Security Token Service (AWS STS) automatically attaches this policy to assumed roles. The identity context is passed as ProvidedContext.

AWSIAMIdentityCenterAllowListForIdentityContext is an [AWS managed policy](#).

Using this policy

You can attach AWSIAMIdentityCenterAllowListForIdentityContext to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 08, 2023, 15:21 UTC
- **Edited time:** June 27, 2024, 19:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
"qapps:PredictQApp",
"qapps:ImportDocument",
"qapps:AssociateLibraryItemReview",
"qapps:DisassociateLibraryItemReview",
"qapps:GetQAppSession",
"qapps:UpdateQAppSession",
"qapps:GetQAppSessionMetadata",
"qapps:UpdateQAppSessionMetadata",
"qapps:TagResource",
"qbusiness:Chat",
```

```
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness>DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIdentitySyncFullAccess

Description: Grants full access to the Identity Sync service

AWSIdentitySyncFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIdentitySyncFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 23, 2022, 23:29 UTC
- **Edited time:** March 23, 2022, 23:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIdentitySyncReadOnlyAccess

Description: Read only access to the Identity Sync service

AWSIdentitySyncReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIdentitySyncReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 23, 2022, 23:29 UTC
- **Edited time:** March 23, 2022, 23:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "identity-sync:GetSyncProfile",
      "identity-sync:ListSyncFilters",
      "identity-sync:GetSyncTarget"
    ],
    "Resource" : "arn:*:identity-sync:*:*:*/*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSImageBuilderFullAccess

Description: Provides full access to all AWS Image Builder actions and resource scoped access to related AWS services.

AWSImageBuilderFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSImageBuilderFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 20, 2019, 18:25 UTC
- **Edited time:** April 13, 2021, 17:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSImageBuilderReadOnlyAccess

Description: Provides read only access to all AWS Image Builder actions.

AWSImageBuilderReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSImageBuilderReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 19, 2019, 22:29 UTC
- **Edited time:** December 19, 2019, 22:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSImportExportFullAccess

Description: Provides read and write access to the jobs created under the AWS account.

AWSImportExportFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSImportExportFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSImportExportFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSImportExportReadOnlyAccess

Description: Provides read only access to the jobs created under the AWS account.

AWSImportExportReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSImportExportReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

Description: Grants Incident Manager permissions to call other AWS services as a part of managing an incident.

AWSIncidentManagerIncidentAccessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSIncidentManagerIncidentAccessServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 13, 2023, 00:01 UTC
- **Edited time:** February 20, 2024, 23:02 UTC
- **ARN:** arn:aws:iam::aws:policy/
AWSIncidentManagerIncidentAccessServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "codedeploy:BatchGetDeployments",
    "codedeploy:ListDeployments",
    "codedeploy:ListDeploymentTargets",
    "autoscaling:DescribeAutoScalingInstances"
  ],
  "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIncidentManagerResolverAccess

Description: This policy grants permissions to start, view, and update incidents with full access to custom timeline events & related items. Assign this policy to users who will create and resolve incidents.

AWSIncidentManagerResolverAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIncidentManagerResolverAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 10, 2021, 06:12 UTC
- **Edited time:** May 10, 2021, 06:12 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIncidentManagerServiceRolePolicy

Description: This policy grants Incident Manager permission to manage incident records and related resources on your behalf.

AWSIncidentManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 10, 2021, 03:34 UTC
- **Edited time:** December 05, 2022, 02:11 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
} ]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoT1ClickFullAccess

Description: Provides full access to AWS IoT 1-Click.

AWSIoT1ClickFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoT1ClickFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2018, 22:10 UTC
- **Edited time:** May 11, 2018, 22:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoT1ClickReadOnlyAccess

Description: Provides read only access to AWS IoT 1-Click.

AWSIoT1ClickReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoT1ClickReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 11, 2018, 21:49 UTC
- **Edited time:** May 11, 2018, 21:49 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTAnalyticsFullAccess

Description: Provides full access to IoT Analytics.

AWSIoTAnalyticsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSIoTAnalyticsFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 18, 2018, 23:02 UTC
- **Edited time:** June 18, 2018, 23:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTAnalyticsReadOnlyAccess

Description: Provides read only access to IoT Analytics.

AWSIoTAnalyticsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTAnalyticsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 18, 2018, 21:37 UTC
- **Edited time:** June 18, 2018, 21:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

```
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTConfigAccess

Description: This policy gives full access to the AWS IoT configuration actions

AWSIoTConfigAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTConfigAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 27, 2015, 21:52 UTC
- **Edited time:** September 27, 2019, 20:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTConfigAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTConfigReadOnlyAccess

Description: This policy gives read only access to the AWS IoT configuration actions

AWSIoTConfigReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTConfigReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 27, 2015, 21:52 UTC
- **Edited time:** September 27, 2019, 20:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDataAccess

Description: This policy gives full access to the AWS IoT messaging actions

AWSIoTDataAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDataAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 27, 2015, 21:51 UTC
- **Edited time:** June 23, 2021, 21:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTDataAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Description: Provides write access to IoT thing groups and read access to IoT Certificates for execution of ADD_THINGS_TO_THING_GROUP mitigation action

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:55 UTC
- **Edited time:** August 07, 2019, 17:55 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderAudit

Description: Provides read access for IoT and related resources

AWSIoTDeviceDefenderAudit is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderAudit to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** July 18, 2018, 21:17 UTC

- **Edited time:** November 25, 2019, 23:52 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Description: Provides access for enabling IoT logging for execution of ENABLE_IOT_LOGGING mitigation action

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:04 UTC
- **Edited time:** August 07, 2019, 17:04 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Description: Provides messages publish access to SNS topic for execution of PUBLISH_FINDING_TO_SNS mitigation action

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:04 UTC
- **Edited time:** August 07, 2019, 17:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Description: Provides write access to IoT policies for execution of REPLACE_DEFAULT_POLICY_VERSION mitigation action

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:04 UTC
- **Edited time:** August 07, 2019, 17:04 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Description: Provides write access to IoT CA certificates for execution of UPDATE_CA_CERTIFICATE mitigation action

AWSIoTDeviceDefenderUpdateCACertMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach `AWSIoTDeviceDefenderUpdateCACertMitigationAction` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:05 UTC
- **Edited time:** August 07, 2019, 17:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Description: Provides write access to IoT certificates for execution of UPDATE_DEVICE_CERTIFICATE mitigation action

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 07, 2019, 17:06 UTC
- **Edited time:** August 07, 2019, 17:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

Description: Allows AWS IoT Device Tester to run the FreeRTOS qualification suite by allowing access to services including IoT, S3, and IAM

AWSIoTDeviceTesterForFreeRTOSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceTesterForFreeRTOSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 12, 2020, 20:33 UTC
- **Edited time:** August 10, 2023, 20:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:::afrc-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:::afrc-ota*",
    "arn:aws:iot:*:*:thinggroup/idx*",
    "arn:aws:iam:*:*:role/idx-*"
  ]
},
{
  "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"
        ]
      }
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTDeviceTesterForGreengrassFullAccess

Description: Allows AWS IoT Device Tester to run the AWS Greengrass qualification suite by allowing access to related services including Lambda, IoT, API Gateway, IAM

AWSIoTDeviceTesterForGreengrassFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTDeviceTesterForGreengrassFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** February 20, 2020, 21:21 UTC
- **Edited time:** June 25, 2020, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTEventsFullAccess

Description: Provides full access to IoT Events.

AWSIoTEventsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTEventsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 10, 2019, 22:51 UTC
- **Edited time:** January 10, 2019, 22:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTEventsReadOnlyAccess

Description: Provides read only access to IoT Events.

AWSIoTEventsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTEventsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 10, 2019, 22:50 UTC
- **Edited time:** September 23, 2019, 17:22 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoT FleetHubFederationAccess

Description: Federation access for IoT Fleet Hub applications

AWSIoT FleetHubFederationAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoT FleetHubFederationAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 15, 2020, 08:08 UTC
- **Edited time:** April 04, 2022, 18:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}

```

```
    "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTfleetwiseServiceRolePolicy

Description: Grants permissions to AWS Resources and metaData used or managed by AWSIoTfleetwise for auxiliary features

AWSIoTfleetwiseServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 21, 2022, 23:27 UTC
- **Edited time:** September 21, 2022, 23:27 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSIoTfleetwiseServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTFullAccess

Description: This policy gives full access to the AWS IoT configuration and messaging actions

AWSIoTFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 08, 2015, 15:19 UTC
- **Edited time:** May 19, 2022, 21:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTLogging

Description: Allows creation of Amazon CloudWatch Log groups and streaming logs to the groups

AWSIoTLogging is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTLogging to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 08, 2015, 15:17 UTC
- **Edited time:** October 08, 2015, 15:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
```

```
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTOTAUpdate

Description: Allows access to create AWS IoT Job and describe the AWS code signer job

AWSIoTOTAUpdate is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTOTAUpdate to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 20, 2017, 20:36 UTC
- **Edited time:** December 20, 2017, 20:36 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTRoboRunnerFullAccess

Description: This policy grants permissions that allow full access to AWS IoT RoboRunner.

AWSIoTRoboRunnerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTRoboRunnerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** November 29, 2021, 03:54 UTC
- **Edited time:** February 23, 2023, 18:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTRoboRunnerReadOnly

Description: This policy grants permissions that allow read-only access to AWS IoT RoboRunner.

AWSIoTRoboRunnerReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTRoboRunnerReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 03:43 UTC
- **Edited time:** November 16, 2022, 20:51 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTRoboRunnerServiceRolePolicy

Description: Allows AWS IoT RoboRunner to manage associated AWS Resources on behalf of the customer.

AWSIoTRoboRunnerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 21, 2023, 16:56 UTC
- **Edited time:** February 21, 2023, 16:56 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTRuleActions

Description: Allows access to all AWS services supported in AWS IoT Rule Actions

AWSIoTRuleActions is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTRuleActions to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 08, 2015, 15:14 UTC
- **Edited time:** January 16, 2018, 19:28 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTSiteWiseConsoleFullAccess

Description: Provides full access to manage AWS IoT SiteWise using the AWS Management Console. Note this policy also grants access to create and list data stores used with AWS IoT SiteWise (e.g. AWS IoT Analytics), access to list and view AWS IoT Greengrass resources, list and modify AWS Secrets Manager secrets, retrieve AWS IoT thing shadows, list resources with specific tags, and create and use a service-linked role for AWS IoT SiteWise.

AWSIoTSiteWiseConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTSiteWiseConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 31, 2019, 21:37 UTC
- **Edited time:** May 31, 2019, 21:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
    }
}

```

```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTSiteWiseFullAccess

Description: Provides full access to IoT SiteWise.

AWSIoTSiteWiseFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTSiteWiseFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 04, 2018, 20:53 UTC
- **Edited time:** December 04, 2018, 20:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTSiteWiseMonitorPortalAccess

Description: This policy grants permissions to access AWS IoT SiteWise assets and asset data, create AWS IoT SiteWise Monitor resources, and list AWS SSO users.

AWSIoTSiteWiseMonitorPortalAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTSiteWiseMonitorPortalAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** May 19, 2020, 20:01 UTC

- **Edited time:** May 19, 2020, 20:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

Description: This role grants AWS IoT SiteWise monitor permissions to access your AWS IoT SiteWise assets & asset properties, and create AWS IoT SiteWise projects, dashboards & access policies through AWS IoT SiteWise portals.

AWSIoTSiteWiseMonitorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 14, 2019, 00:59 UTC
- **Edited time:** December 13, 2019, 22:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTSiteWiseReadOnlyAccess

Description: Provides read only access to IoT SiteWise.

AWSIoTSiteWiseReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTSiteWiseReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 04, 2018, 20:55 UTC
- **Edited time:** September 16, 2022, 19:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTThingsRegistration

Description: This policy allows users to register things at bulk using AWS IoT StartThingRegistrationTask API

AWSIoTThingsRegistration is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTThingsRegistration to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2017, 20:21 UTC
- **Edited time:** October 05, 2020, 19:20 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTtwinMakerServiceRolePolicy

Description: Allows AWS IoT TwinMaker to call other AWS services and to sync their resources on your behalf.

AWSIoTtwinMakerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 13, 2023, 18:59 UTC
- **Edited time:** November 13, 2023, 18:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessDataAccess

Description: Allows the associated identity data access to AWS IoT Wireless devices.

AWSIoTWirelessDataAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSIoTWirelessDataAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:31 UTC
- **Edited time:** December 15, 2020, 15:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessFullAccess

Description: Allows the associated identity full access to all AWS IoT Wireless operations.

AWSIoTWirelessFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTWirelessFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:27 UTC
- **Edited time:** December 15, 2020, 15:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessFullPublishAccess

Description: Provides IoT Wireless full access to publish to IoT Rules Engine on your behalf.

AWSIoTWirelessFullPublishAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTWirelessFullPublishAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:29 UTC
- **Edited time:** December 15, 2020, 15:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessGatewayCertManager

Description: Allows the associated identity access to create, list and describe IoT Certificates

AWSIoTWirelessGatewayCertManager is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTWirelessGatewayCertManager to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:30 UTC
- **Edited time:** December 15, 2020, 15:30 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessLogging

Description: Allows the associated identity to create Amazon CloudWatch Logs groups and stream logs to the groups.

AWSIoTWirelessLogging is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTWirelessLogging to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:32 UTC
- **Edited time:** December 15, 2020, 15:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTWirelessLogging

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIoTWirelessReadOnlyAccess

Description: Allows the associated identity read only access to AWS IoT wireless.

AWSIoTWirelessReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIoTWirelessReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 15, 2020, 15:28 UTC
- **Edited time:** December 15, 2020, 15:28 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIPAMServiceRolePolicy

Description: Allows VPC IP Address Manager to access VPC resources and integrate with AWS Organizations on your behalf.

AWSIPAMServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 30, 2021, 19:08 UTC

- **Edited time:** November 08, 2023, 19:05 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIQContractServiceRolePolicy

Description: Used by AWS IQ to execute payment requests on behalf of a customer

AWSIQContractServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 22, 2019, 19:28 UTC
- **Edited time:** August 22, 2019, 19:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIQFullAccess

Description: Provides full access to AWS IQ

AWSIQFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSIQFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 04, 2019, 23:13 UTC
- **Edited time:** September 25, 2019, 20:22 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSIQFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSIQPermissionServiceRolePolicy

Description: Allows AWS IQ to manage the role assumed by AWS IQ experts.

AWSIQPermissionServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 22, 2019, 19:36 UTC
- **Edited time:** August 22, 2019, 19:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Description: Enables access to AWS services and resources required for AWS KMS custom key stores

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 14, 2018, 20:10 UTC
- **Edited time:** November 10, 2023, 19:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Description: Enables AWS KMS to synchronize the shared properties of multi-Region keys.

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 16, 2021, 15:37 UTC
- **Edited time:** June 16, 2021, 15:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSKeyManagementServicePowerUser

Description: Provides access to AWS Key Management Service (KMS).

AWSKeyManagementServicePowerUser is an [AWS managed policy](#).

Using this policy

You can attach AWSKeyManagementServicePowerUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** March 07, 2017, 00:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLakeFormationCrossAccountManager

Description: Provides cross account access to Glue resources via Lake Formation. Also grants read access to other required services such as organizations and resource access manager

AWSLakeFormationCrossAccountManager is an [AWS managed policy](#).

Using this policy

You can attach AWSLakeFormationCrossAccountManager to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 04, 2020, 20:59 UTC
- **Edited time:** March 22, 2024, 18:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLakeFormationDataAdmin

Description: Grants administrative access to AWS Lake Formation and related services, such as AWS Glue, to manage data lakes

AWSLakeFormationDataAdmin is an [AWS managed policy](#).

Using this policy

You can attach AWSLakeFormationDataAdmin to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 08, 2019, 17:33 UTC
- **Edited time:** March 22, 2024, 18:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambda_FullAccess

Description: Grants full access to AWS Lambda service, AWS Lambda console features, and other related AWS services.

AWSLambda_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSLambda_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2020, 21:14 UTC
- **Edited time:** November 17, 2020, 21:14 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLambda_FullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}

```



```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambda_ReadOnlyAccess

Description: Grants read-only access to AWS Lambda service, AWS Lambda console features, and other related AWS services.

AWSLambda_ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSLambda_ReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2020, 21:10 UTC
- **Edited time:** July 27, 2023, 17:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaBasicExecutionRole

Description: Provides write permissions to CloudWatch Logs.

AWSLambdaBasicExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaBasicExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 09, 2015, 15:03 UTC
- **Edited time:** April 09, 2015, 15:03 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaDynamoDBExecutionRole

Description: Provides list and read access to DynamoDB streams and write permissions to CloudWatch logs.

AWSLambdaDynamoDBExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaDynamoDBExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 09, 2015, 15:09 UTC
- **Edited time:** April 09, 2015, 15:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaENIManagementAccess

Description: Provides minimum permissions for a Lambda function to manage ENIs (create, describe, delete) used by a VPC-enabled Lambda Function.

AWSLambdaENIManagementAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaENIManagementAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 06, 2016, 00:37 UTC
- **Edited time:** October 01, 2020, 20:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaExecute

Description: Provides Put, Get access to S3 and full access to CloudWatch Logs.

AWSLambdaExecute is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaExecute to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLambdaExecute

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaFullAccess

Description: This policy is on a deprecation path. See documentation for guidance: <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>. Provides full access to Lambda, S3, DynamoDB, CloudWatch Metrics and Logs.

AWSLambdaFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 27, 2017, 23:22 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSLambdaFullAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaInvocation-DynamoDB

Description: Provides read access to DynamoDB Streams.

AWSLambdaInvocation-DynamoDB is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaInvocation-DynamoDB to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** February 06, 2015, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaKinesisExecutionRole

Description: Provides list and read access to Kinesis streams and write permissions to CloudWatch logs.

AWSLambdaKinesisExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach `AWSLambdaKinesisExecutionRole` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 09, 2015, 15:14 UTC
- **Edited time:** November 19, 2018, 20:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaMSKExecutionRole

Description: Provides permissions required to access MSK Cluster within a VPC, manage ENIs (create, describe, delete) in the VPC and write permissions to CloudWatch Logs.

AWSLambdaMSKExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaMSKExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 11, 2020, 17:35 UTC
- **Edited time:** August 02, 2022, 20:08 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaReplicator

Description: Grants Lambda Replicator necessary permissions to replicate functions across regions

AWSLambdaReplicator is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 23, 2017, 17:53 UTC
- **Edited time:** December 08, 2017, 00:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaRole

Description: Default policy for AWS Lambda service role.

AWSLambdaRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaSQSQueueExecutionRole

Description: Provides receive message, delete message, and read attribute access to SQS queues, and write permissions to CloudWatch logs.

AWSLambdaSQSQueueExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaSQSQueueExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 14, 2018, 21:50 UTC
- **Edited time:** June 14, 2018, 21:50 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLambdaVPCAccessExecutionRole

Description: Provides minimum permissions for a Lambda function to execute while accessing a resource within a VPC - create, describe, delete network interfaces and write permissions to CloudWatch Logs.

AWSLambdaVPCAccessExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach AWSLambdaVPCAccessExecutionRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 11, 2016, 23:15 UTC
- **Edited time:** January 05, 2024, 22:38 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerConsumptionPolicy

Description: Provides permissions to allow access to the AWS License Manager API actions required to consume upon licenses that the user has entitlements.

AWSLicenseManagerConsumptionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSLicenseManagerConsumptionPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 11, 2021, 23:18 UTC
- **Edited time:** August 11, 2021, 23:18 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Description: Allows AWS License Manager Linux Subscriptions Service to manage resources on your behalf.

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 20, 2022, 18:54 UTC
- **Edited time:** December 20, 2022, 18:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerMasterAccountRolePolicy

Description: AWS License Manager service master account role policy

AWSLicenseManagerMasterAccountRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2018, 19:03 UTC
- **Edited time:** May 31, 2022, 20:50 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerMemberAccountRolePolicy

Description: AWS License Manager service member account role policy

AWSLicenseManagerMemberAccountRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** November 26, 2018, 19:04 UTC
- **Edited time:** November 15, 2019, 22:09 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerServiceRolePolicy

Description: AWS License Manager service default role policy

AWSLicenseManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2018, 19:02 UTC
- **Edited time:** July 30, 2021, 01:43 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Description: Allows AWS License Manager User Subscriptions Service to manage resources on your behalf.

AWSLicenseManagerUserSubscriptionsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** July 30, 2022, 01:17 UTC
- **Edited time:** November 21, 2022, 19:51 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSM2ServicePolicy

Description: Allows AWS M2 to manage AWS resources on your behalf.

AWSM2ServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 07, 2022, 20:26 UTC
- **Edited time:** June 07, 2022, 20:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedServices_ContactsServiceRolePolicy

Description: Allows AWS Managed Services to read the values of the tags on AWS resources

AWSManagedServices_ContactsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 23, 2023, 17:07 UTC
- **Edited time:** March 23, 2023, 17:07 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Description: AWS Managed Services - policy to manage detective controls infrastructure

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 19, 2022, 23:11 UTC
- **Edited time:** December 19, 2022, 23:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedServices_EventsServiceRolePolicy

Description: AWS Managed Services policy to enable AMS event processor feature.

AWSManagedServices_EventsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 07, 2023, 18:41 UTC
- **Edited time:** February 07, 2023, 18:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedServicesDeploymentToolkitPolicy

Description: Allows AWS Managed Services to manage deployment toolkit on your behalf.

AWSManagedServicesDeploymentToolkitPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 09, 2022, 18:33 UTC
- **Edited time:** April 04, 2024, 20:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceAmiIngestion

Description: Allows AWS Marketplace to copy your Amazon Machine Images (AMIs) in order to list them on AWS Marketplace

AWSMarketplaceAmiIngestion is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceAmiIngestion to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 25, 2020, 20:55 UTC
- **Edited time:** September 25, 2020, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceDeploymentServiceRolePolicy

Description: Allows AWS Marketplace to create and manage seller deployment parameters for the products that you subscribe to on AWS Marketplace.

AWSMarketplaceDeploymentServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 15, 2023, 23:34 UTC
- **Edited time:** November 15, 2023, 23:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceFullAccess

Description: Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows users to manage Marketplace software instances from the Marketplace 'Your Software' page, and provides administrative access to EC2.

AWSMarketplaceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 11, 2015, 17:21 UTC
- **Edited time:** March 04, 2022, 17:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceGetEntitlements

Description: Provides read access to AWS Marketplace Entitlements

AWSMarketplaceGetEntitlements is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceGetEntitlements to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 27, 2017, 19:37 UTC
- **Edited time:** April 05, 2024, 01:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceImageBuildFullAccess

Description: Provides full access to AWS Marketplace Private Image Build Feature. In addition to create private images, it also provides permissions to add tags to images, launch and terminate ec2 instances.

AWSMarketplaceImageBuildFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceImageBuildFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 31, 2018, 23:29 UTC
- **Edited time:** March 04, 2022, 17:05 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by AWS Marketplace for license management.

AWSMarketplaceLicenseManagementServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 03, 2020, 08:33 UTC
- **Edited time:** December 03, 2020, 08:33 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceManageSubscriptions

Description: Provides the ability to subscribe and unsubscribe to AWS Marketplace software

AWSMarketplaceManageSubscriptions is an [AWS managed policy](#).

Using this policy

You can attach `AWSMarketplaceManageSubscriptions` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** January 19, 2023, 23:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceMeteringFullAccess

Description: Provides full access to AWS Marketplace Metering.

AWSMarketplaceMeteringFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceMeteringFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 17, 2016, 22:39 UTC
- **Edited time:** March 17, 2016, 22:39 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceMeteringRegisterUsage

Description: Provides permissions to register a resource and track usage through AWS Marketplace Metering Service.

AWSMarketplaceMeteringRegisterUsage is an [AWS managed policy](#).

Using this policy

You can attach `AWSMarketplaceMeteringRegisterUsage` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 21, 2019, 01:17 UTC
- **Edited time:** November 21, 2019, 01:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceProcurementSystemAdminFullAccess

Description: Provides full access to all administrative actions for an AWS Marketplace eProcurement integration.

AWSMarketplaceProcurementSystemAdminFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceProcurementSystemAdminFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 25, 2019, 13:07 UTC
- **Edited time:** June 25, 2019, 13:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:PutProcurementSystemConfiguration",
    "aws-marketplace:DescribeProcurementSystemConfiguration",
    "organizations:Describe*",
    "organizations:List*"
  ],
  "Resource" : [
    "*"
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

Description: Enables access for AWS Marketplace services to purchase order management.

AWSMarketplacePurchaseOrdersServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 27, 2021, 15:12 UTC
- **Edited time:** October 27, 2021, 15:12 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceRead-only

Description: Provides the ability to review AWS Marketplace subscriptions

AWSMarketplaceRead-only is an [AWS managed policy](#).

Using this policy

You can attach `AWSMarketplaceRead-only` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** January 19, 2023, 23:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by AWS Marketplace for Resale Authorization.

AWSMarketplaceResaleAuthorizationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 05, 2024, 18:47 UTC
- **Edited time:** March 05, 2024, 18:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceSellerFullAccess

Description: Provides full access to all seller operations on the AWS Marketplace and other AWS services such as AMI management.

AWSMarketplaceSellerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceSellerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 02, 2019, 20:40 UTC
- **Edited time:** March 15, 2024, 16:09 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]

```



```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceSellerProductsFullAccess

Description: Provides sellers full access to AWS Marketplace Management Products page and other AWS services such as AMI management.

AWSMarketplaceSellerProductsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceSellerProductsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 02, 2019, 21:06 UTC
- **Edited time:** July 18, 2023, 22:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMarketplaceSellerProductsReadOnly

Description: Provide sellers read-only access to AWS Marketplace Management Products page.

AWSMarketplaceSellerProductsReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSMarketplaceSellerProductsReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 02, 2019, 21:40 UTC
- **Edited time:** November 19, 2022, 00:08 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMediaConnectServicePolicy

Description: The default policy that enables access to AWS services and Resources used or managed by MediaConnect.

AWSMediaConnectServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 03, 2023, 22:11 UTC

- **Edited time:** April 03, 2023, 22:11 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMediaTailorServiceRolePolicy

Description: Enable access to AWS Resources used or managed by MediaTailor

AWSMediaTailorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** September 17, 2021, 22:27 UTC
- **Edited time:** September 17, 2021, 22:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubDiscoveryAccess

Description: Policy allows AWSMigrationHubService to call AWSApplicationDiscoveryService on behalf of the customer.

AWSMigrationHubDiscoveryAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubDiscoveryAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 13:30 UTC
- **Edited time:** August 06, 2020, 17:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubDMSAccess

Description: Policy for Database Migration Service to assume role in customer's account to call Migration Hub

AWSMigrationHubDMSAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubDMSAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 14:00 UTC
- **Edited time:** October 07, 2019, 17:51 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubFullAccess

Description: Managed policy to provide the customer access to the Migration Hub Service

AWSMigrationHubFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 14, 2017, 14:02 UTC
- **Edited time:** June 19, 2019, 21:14 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubOrchestratorConsoleFullAccess

Description: Provides limited access to AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service and AWS Secrets Manager. This policy also grants full access to AWS Migration Hub Orchestrator service.

AWSMigrationHubOrchestratorConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubOrchestratorConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 20, 2022, 02:26 UTC
- **Edited time:** December 05, 2023, 17:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

Description: This policy needs to be attached for SAP and MGN migrated instance for our service to orchestrate instances by downloading scripts from S3 and to fetch secret values inside EC2 instance.

AWSMigrationHubOrchestratorInstanceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubOrchestratorInstanceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 20, 2022, 02:43 UTC
- **Edited time:** April 20, 2022, 02:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubOrchestratorPlugin

Description: Provides limited access to Amazon Simple Storage Service, AWS Secrets Manager and Plugin related actions for AWS Migration Hub Orchestrator.

AWSMigrationHubOrchestratorPlugin is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubOrchestratorPlugin to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 20, 2022, 02:25 UTC

- **Edited time:** April 20, 2022, 02:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubOrchestratorServiceRolePolicy

Description: Provides permissions necessary for Migration Hub Orchestrator to migrate and modernize your on-premises workloads

AWSMigrationHubOrchestratorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 20, 2022, 02:24 UTC
- **Edited time:** March 04, 2024, 18:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Description: Grants full access to AWS Migration Hub Refactor Spaces and other AWS related services except AWS Transit Gateway and EC2 security groups not required when using environments without a network bridge. This policy also excludes permissions required for AWS Lambda and AWS Resource Access Manager as they can be scoped down based on tags.

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 03, 2023, 20:09 UTC
- **Edited time:** April 11, 2024, 18:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Description: Use in the IAM service role passed to the SSM Automation document AWSRefactorSpaces-CreateResources to grant permissions required to run the automation. The policy grants read/write access to EC2 tags in order to track automation progress. When the Refactor Spaces environment's network bridge is enabled, the automation also adds the environment's security group to the EC2 instance to permit traffic from other Refactor Spaces services in the environment. The policy also grants access to the Application Migration Service's post launch actions SSM parameters.

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubRefactorSpaces-SSMAutomationPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 10, 2023, 15:08 UTC
- **Edited time:** August 10, 2023, 15:08 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-
*"
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubRefactorSpacesFullAccess

Description: Grants full access to AWS MigrationHub Refactor Spaces, AWS MigrationHub Refactor Spaces console features and other related AWS services except permissions required for AWS Lambda and AWS Resource Access Manager as they can be scoped down based on tags.

AWSMigrationHubRefactorSpacesFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubRefactorSpacesFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2021, 07:12 UTC
- **Edited time:** April 11, 2024, 17:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-
n1b-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:application-id" : "false"
      }
    }
  }
},
{
  "Sid" : "ELBDescribe",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeListeners"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ELBModify",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:CreateLoadBalancerListeners",
    "elasticloadbalancing:CreateListener",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/refactor-spaces:route-id" : [
        "*"
      ]
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "ELBLoadBalancerDelete",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DeleteLoadBalancer",
  "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
},
{
  "Sid" : "ELBListenerCreate",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateListener"
  ],
  "Resource" : [
    "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
    "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "Sid" : "ELBListenerDelete",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
},
{
  "Sid" : "ELBTargetGroupModify",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DeleteTargetGroup",
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
},
{
  "Sid" : "ELBTargetGroupCreate",
```



```

    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateTargetGroup"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Sid" : "APIGatewayModify",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:DELETE",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:UpdateRestApiPolicy"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*",
      "arn:aws:apigateway:*:*/vpclinks",
      "arn:aws:apigateway:*:*/vpclinks/*",
      "arn:aws:apigateway:*:*/tags",
      "arn:aws:apigateway:*:*/tags/*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Sid" : "APIGatewayVpcLinksGet",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*:*/vpclinks",
      "arn:aws:apigateway:*:*/vpclinks/*"
    ]
  }
}

```

```
]
},
{
  "Sid" : "OrganizationDescribe",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudformationStackCreate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudformationStackTag",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:TagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/*"
},
{
  "Sid" : "CreateRefactorSpacesSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
    }
  }
},
{
  "Sid" : "CreateELBSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
```

```
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

Description: Provides access to AWS Resources managed or used by AWS Migration Hub Refactor Spaces.

AWSMigrationHubRefactorSpacesServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2021, 06:50 UTC
- **Edited time:** July 20, 2023, 15:57 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2>DeleteTags",
        "ram>DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:CreateLoadBalancerListeners",
    "elasticloadbalancing:CreateListener",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/refactor-spaces:route-id" : [
        "*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:PUT",
    "apigateway:POST",
    "apigateway:GET",
    "apigateway:PATCH",
    "apigateway:DELETE"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/vpclinks/*",

```

```

    "arn:aws:apigateway:*::/tags",
    "arn:aws:apigateway:*::/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DeleteLoadBalancer",
  "Resource" : "arn:*:elasticloadbalancing:*::loadbalancer/net/refactor-spaces-
nlb-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateListener"
  ],
  "Resource" : [
    "arn:*:elasticloadbalancing:*::loadbalancer/net/refactor-spaces-nlb-*",
    "arn:*:elasticloadbalancing:*::listener/net/refactor-spaces-nlb-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*::listener/net/refactor-spaces-nlb-*"
},
{
  "Effect" : "Allow",
  "Action" : [

```

```
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn::*:elasticloadbalancing::*:targetgroup/refactor-spaces-tg-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:DeregisterTargets"
    ],
    "Resource" : "arn::*:elasticloadbalancing::*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
    ],
    "Resource" : "arn::*:elasticloadbalancing::*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
    }
}
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubSMSAccess

Description: Policy for Server Migration Service to assume role in customer's account to call Migration Hub

AWSMigrationHubSMSAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubSMSAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 14, 2017, 13:57 UTC
- **Edited time:** October 07, 2019, 18:01 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubStrategyCollector

Description: Grants permissions to allow communication with the AWS Migration Hub Strategy Recommendations service, read/write access to S3 buckets related to the service, Amazon API Gateway access to upload logs and metrics to AWS, AWS Secrets Manager access to fetch credentials, and any related services.

AWSMigrationHubStrategyCollector is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubStrategyCollector to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 19, 2021, 20:15 UTC
- **Edited time:** April 01, 2024, 16:21 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubStrategyConsoleFullAccess

Description: Grants full access to the AWS Migration Hub Strategy Recommendations service and access to related AWS services through the AWS Management Console.

AWSMigrationHubStrategyConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMigrationHubStrategyConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 19, 2021, 20:13 UTC
- **Edited time:** November 09, 2022, 00:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMigrationHubStrategyServiceRolePolicy

Description: Enable access to AWS Resources used or managed by AWS Migration Hub Strategy Recommendations service.

AWSMigrationHubStrategyServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 19, 2021, 20:02 UTC

- **Edited time:** October 19, 2021, 20:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMobileHub_FullAccess

Description: This policy may be attached to any User, Role, or Group, in order to grant users permission to create, delete, and modify projects (and their associated AWS resources) in AWS Mobile Hub. This also includes permissions to generate and download sample mobile app source code for each Mobile Hub project.

AWSMobileHub_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSMobileHub_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 05, 2016, 19:56 UTC
- **Edited time:** December 19, 2019, 23:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMobileHub_ReadOnly

Description: This policy may be attached to any User, Role, or Group, in order to grant users permission to list and view projects in AWS Mobile Hub. This also includes permissions to generate and download sample mobile app source code for each Mobile Hub project. It does not allow the user to modify any configuration for any Mobile Hub project.

AWSMobileHub_ReadOnly is an [AWS managed policy](#).

Using this policy

You can attach `AWSMobileHub_ReadOnly` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 05, 2016, 19:55 UTC
- **Edited time:** July 23, 2018, 21:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSMSKReplicatorExecutionRole

Description: Grants permissions to Amazon MSK Replicator to replicate data between MSK Clusters.

AWSMSKReplicatorExecutionRole is an [AWS managed policy](#).

Using this policy

You can attach `AWSMSKReplicatorExecutionRole` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 06, 2023, 00:07 UTC
- **Edited time:** March 25, 2024, 21:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSNetworkFirewallServiceRolePolicy

Description: Allow AWSNetworkFirewall to create and manage necessary resources for your Firewalls.

AWSNetworkFirewallServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 17, 2020, 17:17 UTC
- **Edited time:** March 30, 2023, 17:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```



```

    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "acm:DescribeCertificate",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "resource-groups:ListGroupResources",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "tag:GetResources",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "resource-groups.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint",
      "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [

```

```
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
    }
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSNetworkManagerCloudWANServiceRolePolicy

Description: Allow NetworkManager to access resources associated with your Core Network

AWSNetworkManagerCloudWANServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 12, 2022, 12:17 UTC
- **Edited time:** July 12, 2022, 12:17 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSNetworkManagerFullAccess

Description: Provides full access to Amazon NetworkManager via the AWS Management Console.

AWSNetworkManagerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSNetworkManagerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 17:37 UTC
- **Edited time:** December 03, 2019, 17:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSNetworkManagerReadOnlyAccess

Description: Provides read only access to Amazon NetworkManager via the AWS Management Console.

AWSNetworkManagerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSNetworkManagerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 03, 2019, 17:35 UTC
- **Edited time:** December 03, 2019, 17:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "networkmanager:Describe*",
      "networkmanager:Get*",
      "networkmanager:List*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSNetworkManagerServiceRolePolicy

Description: Allow NetworkManager to access resources associated with your Global Networks

AWSNetworkManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 03, 2019, 14:03 UTC
- **Edited time:** July 27, 2022, 19:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorks_FullAccess

Description: Provides full access to AWS OpsWorks.

AWSOpsWorks_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorks_FullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 22, 2021, 16:29 UTC
- **Edited time:** January 22, 2021, 16:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksCloudWatchLogs

Description: Enables OpsWorks instances with the CWLogs integration enabled to ship logs and create required log groups

AWSOpsWorksCloudWatchLogs is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksCloudWatchLogs to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 30, 2017, 17:47 UTC
- **Edited time:** March 30, 2017, 17:47 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksCMInstanceProfileRole

Description: Provides S3 access for instances launched by OpsWorks CM.

AWSOpsWorksCMInstanceProfileRole is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksCMInstanceProfileRole to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 24, 2016, 09:48 UTC
- **Edited time:** April 23, 2021, 17:34 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksCMServiceRole

Description: Service Role Policy to be used for Creating OpsWorks CM servers.

AWSOpsWorksCMServiceRole is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksCMServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 24, 2016, 09:49 UTC
- **Edited time:** April 23, 2021, 17:32 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksInstanceRegistration

Description: Provides access for an Amazon EC2 instance to register with an AWS OpsWorks stack.

AWSOpsWorksInstanceRegistration is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksInstanceRegistration to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 03, 2016, 14:23 UTC
- **Edited time:** June 03, 2016, 14:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksRegisterCLI_EC2

Description: Policy to enable registration of EC2 instances via the OpsWorks CLI

AWSOpsWorksRegisterCLI_EC2 is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksRegisterCLI_EC2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 18, 2019, 15:56 UTC
- **Edited time:** June 18, 2019, 15:56 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOpsWorksRegisterCLI_OnPremises

Description: Policy to enable registration of On-Premises instances via the OpsWorks CLI

AWSOpsWorksRegisterCLI_OnPremises is an [AWS managed policy](#).

Using this policy

You can attach AWSOpsWorksRegisterCLI_OnPremises to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 18, 2019, 15:33 UTC
- **Edited time:** June 18, 2019, 15:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOrganizationsFullAccess

Description: Provides full access to AWS Organizations.

AWSOrganizationsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSOrganizationsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 06, 2018, 20:31 UTC
- **Edited time:** February 06, 2024, 17:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOrganizationsReadOnlyAccess

Description: Provides read-only access to AWS Organizations.

AWSOrganizationsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSOrganizationsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 06, 2018, 20:32 UTC
- **Edited time:** June 07, 2024, 21:32 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWS Organizations Service Trust Policy

Description: A policy to allow AWS Organizations to share trust with other approved AWS services for the purpose of simplifying customer configuration.

AWS Organizations Service Trust Policy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 10, 2017, 23:04 UTC
- **Edited time:** November 01, 2017, 06:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOutpostsAuthorizeServerPolicy

Description: This policy grants permissions that allow you to install an Outpost server on your on-premises network.

AWSOutpostsAuthorizeServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSOutpostsAuthorizeServerPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 04, 2023, 19:23 UTC

- **Edited time:** January 04, 2023, 19:23 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSOutpostsServiceRolePolicy

Description: Service Linked Role policy to enable access to AWS resources managed by AWS Outposts

AWSOutpostsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 09, 2020, 22:55 UTC
- **Edited time:** November 09, 2020, 22:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaApplianceRolePolicy

Description: Allows AWS IoT software on an AWS Panorama Appliance to upload logs to Amazon CloudWatch.

AWSPanoramaApplianceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaApplianceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2020, 13:13 UTC
- **Edited time:** December 01, 2020, 13:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaApplianceServiceRolePolicy

Description: Allows an AWS Panorama Appliance to upload logs to Amazon CloudWatch, and to get objects from Amazon S3 access points created for use with AWS Panorama.

AWSPanoramaApplianceServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaApplianceServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** October 20, 2021, 12:14 UTC

- **Edited time:** January 17, 2023, 21:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaFullAccess

Description: Provides full access to AWS Panorama

AWSPanoramaFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2020, 13:12 UTC
- **Edited time:** January 12, 2022, 21:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaGreengrassGroupRolePolicy

Description: Allows an AWS Lambda function on an AWS Panorama Appliance to manage resources in Panorama, upload logs and metrics to Amazon CloudWatch, and to manage objects in buckets created for use with Panorama.

AWSPanoramaGreengrassGroupRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaGreengrassGroupRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2020, 13:10 UTC
- **Edited time:** January 06, 2021, 19:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaSageMakerRolePolicy

Description: Allows Amazon SageMaker to manage objects in buckets created for use with AWS Panorama.

AWSPanoramaSageMakerRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaSageMakerRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2020, 13:13 UTC
- **Edited time:** December 01, 2020, 13:13 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaServiceLinkedRolePolicy

Description: Allows AWS Panorama to manage resources in AWS IoT, AWS Secrets Manager and AWS Panorama.

AWSPanoramaServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 20, 2021, 12:12 UTC
- **Edited time:** October 20, 2021, 12:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPanoramaServiceRolePolicy

Description: Allows AWS Panorama to manage resources in Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda, Amazon SageMaker, and Amazon CloudWatch Logs, and to pass service roles to AWS IoT, AWS IoT GreenGrass, and Amazon SageMaker.

AWSPanoramaServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPanoramaServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 01, 2020, 13:14 UTC
- **Edited time:** December 01, 2020, 13:14 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPriceListServiceFullAccess

Description: Provides full access to AWS Price List Service.

AWSPriceListServiceFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSPriceListServiceFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 22, 2017, 00:36 UTC
- **Edited time:** November 22, 2017, 00:36 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPRivateCAAuditor

Description: Provides auditor access to AWS Private Certificate Authority

AWSPRivateCAAuditor is an [AWS managed policy](#).

Using this policy

You can attach AWSPRivateCAAuditor to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 14, 2023, 18:33 UTC
- **Edited time:** February 14, 2023, 18:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSPRivateCAAuditor

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPrivateCAFullAccess

Description: Provides full access to AWS Private Certificate Authority

AWSPriateCAFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSPriateCAFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 14, 2023, 18:20 UTC
- **Edited time:** February 14, 2023, 18:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSPriateCAFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPRivateCAPrivilegedUser

Description: Provides privileged certificate user access to AWS Private Certificate Authority

AWSPRivateCAPrivilegedUser is an [AWS managed policy](#).

Using this policy

You can attach AWSPRivateCAPrivilegedUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 14, 2023, 18:26 UTC
- **Edited time:** February 14, 2023, 18:26 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSPRivateCAPrivilegedUser

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPRivateCARedOnly

Description: Provides read only access to AWS Private Certificate Authority

AWSPRivateCARedOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSPRivateCARedOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 14, 2023, 18:30 UTC
- **Edited time:** February 14, 2023, 18:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSPRivateCARedOnly`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPriateCAUser

Description: Provides certificate user access to AWS Private Certificate Authority

AWSPriateCAUser is an [AWS managed policy](#).

Using this policy

You can attach AWSPriateCAUser to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 14, 2023, 18:16 UTC
- **Edited time:** February 14, 2023, 18:16 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSPriateCAUser

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPrivateMarketplaceAdminFullAccess

Description: Provides full access to all administrative actions for an AWS Private Marketplace.

AWSPrivateMarketplaceAdminFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSPrivateMarketplaceAdminFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 16:32 UTC
- **Edited time:** February 14, 2024, 22:05 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPrivateMarketplaceRequests

Description: Provides access to creating requests in an AWS Private Marketplace.

AWSPrivateMarketplaceRequests is an [AWS managed policy](#).

Using this policy

You can attach `AWSPRivateMarketplaceRequests` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 28, 2019, 21:44 UTC
- **Edited time:** October 28, 2019, 21:44 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSPRivateMarketplaceRequests`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPrivateNetworksServiceRolePolicy

Description: Allows AWS Private Networks Service to manage resources on behalf of the customer.

AWSPrivateNetworksServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 16, 2021, 23:17 UTC
- **Edited time:** December 16, 2021, 23:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
"Action" : [
  "cloudwatch:PutMetricData"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "cloudwatch:namespace" : "AWS/Private5G"
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonCodeBuildProvisioningBasicAccess

Description: Permissions CodeBuild needs to run a build for AWS Proton CodeBuild Provisioning.

AWSProtonCodeBuildProvisioningBasicAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSProtonCodeBuildProvisioningBasicAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 09, 2022, 21:04 UTC
- **Edited time:** November 09, 2022, 21:04 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

Description: Allows AWS Proton to manage Proton resource provisioning using CodeBuild and other AWS services on your behalf.

AWSProtonCodeBuildProvisioningServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 09, 2022, 21:32 UTC
- **Edited time:** May 17, 2023, 16:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonDeveloperAccess

Description: Provides access to the AWS Proton APIs and Management Console, but does not allow administration of Proton templates or environments.

AWSProtonDeveloperAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSProtonDeveloperAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 17, 2021, 19:02 UTC
- **Edited time:** June 06, 2024, 18:26 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonFullAccess

Description: Provides full access to the AWS Proton APIs and Management Console. In addition to these permissions, access to Amazon S3 is also needed to register template bundles from your S3 buckets, as well as access to Amazon IAM to create and manage the service roles for Proton.

AWSProtonFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSProtonFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 17, 2021, 19:07 UTC
- **Edited time:** June 06, 2024, 18:29 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSProtonFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonReadOnlyAccess

Description: Provides read only access to the AWS Proton APIs and Management Console.

AWSProtonReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSProtonReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 17, 2021, 19:09 UTC
- **Edited time:** November 18, 2022, 18:28 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonServiceGitSyncServiceRolePolicy

Description: Policy which allows AWS Proton to sync your service, environment and component definitions from your git repository to AWS Proton.

AWSProtonServiceGitSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 04, 2023, 15:55 UTC
- **Edited time:** April 04, 2023, 15:55 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSProtonSyncServiceRolePolicy

Description: Policy which allows AWS Proton to sync your git repository contents to Proton or sync Proton contents to your git repositories.

AWSProtonSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 23, 2021, 21:14 UTC
- **Edited time:** May 05, 2024, 01:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSPurchaseOrdersServiceRolePolicy

Description: Grants permissions to view and modify purchase orders on billing console

AWSPurchaseOrdersServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSPurchaseOrdersServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 06, 2020, 18:15 UTC
- **Edited time:** July 17, 2023, 18:59 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupCFGCPacksPermissionsBoundary

Description: The AWSQuickSetupCFGCPacksPermissionsBoundary policy defines the list of permissions that are permitted in an IAM role created by Quick Setup. Quick Setup uses a role created with this policy to deploy AWS Config conformance packs.

AWSQuickSetupCFGCPacksPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupCFGCPacksPermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:52 UTC
- **Edited time:** June 26, 2024, 09:52 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
```

```

    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "PutCPackPermissions",
    "Effect" : "Allow",
    "Action" : [
      "config:PutConformancePack"
    ],
    "Resource" : [
      "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : [
          "${aws:PrincipalAccount}"
        ]
      }
    }
  },
  {
    "Sid" : "DescribeCPacksPermissions",
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeConformancePackStatus"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConformancePacksSLRCreatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    ],
    "Condition" : {
      "StringEquals" : {

```

```

        "iam:AWSServiceName" : "config-conforms.amazonaws.com"
    }
}
},
{
    "Sid" : "SystemsManagerSLRCreatePermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
    }
},
{
    "Sid" : "EnableExplorerReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
    "Effect" : "Allow",
    "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
    ],
    "Resource" : [
        "arn:aws:ssm::*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm::*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm::*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm::*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm::*:servicesetting/ssm/opsdata/ComputeOptimizer",

```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
    ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupDeploymentRolePolicy

Description: Provides permissions for AWS Systems Manager Quick Setup to deploy multiple configuration types. These configuration types create IAM roles and automations that configure frequently used Amazon Web Services services and features with recommended best practices.

AWSQuickSetupDeploymentRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupDeploymentRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:55 UTC
- **Edited time:** June 26, 2024, 09:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",

```

```
"Action" : [
  "resource-groups:GetGroupQuery"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "CPacksRead",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConformancePacks",
    "config:DescribeConformancePackStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OpsPacksManage",
  "Effect" : "Allow",
  "Action" : [
    "config:PutConformancePack",
    "config>DeleteConformancePack"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  },
  "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
},
{
  "Sid" : "QSDocsManage",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateDocument",
    "ssm:UpdateDocument",
    "ssm:UpdateDocumentDefaultVersion",
    "ssm>DeleteDocument",
    "ssm:AddTagsToResource",
    "ssm:RemoveTagsFromResource",
    "ssm:ListTagsForResource"
  ],
}
```

```
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "cloudformation.amazonaws.com"
    ]
  }
},
"Resource" : [
  "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
  "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
  "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
],
{
  "Sid" : "QSDocsRead",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetDocument"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
    "arn:aws:ssm:*:*:document/AWSOperationsPack*",
    "arn:aws:ssm:*:*:document/AWSConformancePacks-*",
    "arn:aws:ssm:*:*:document/AWSEC2-UpdateLaunchAgent",
    "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:document/AWS-RunPatchBaselineAssociation",
    "arn:aws:ssm:*:*:document/AWS-UpdateSSMAgent"
  ]
},
{
  "Sid" : "QSAssociationsManage",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm:UpdateAssociation",
    "ssm>DeleteAssociation",
    "ssm:DescribeAssociation"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
```

```

    ]
  }
},
"Resource" : [
  "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
  "arn:aws:ssm:*:*:document/AWSOperationsPack*",
  "arn:aws:ssm:*:*:document/AWSEC2-UpdateLaunchAgent",
  "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
  "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
  "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
  "arn:aws:ssm:*:*:document/AWS-RunPatchBaselineAssociation",
  "arn:aws:ssm:*:*:document/AWS-UpdateSSMAgent",
  "arn:aws:ec2:*:*:instance/*",
  "arn:aws:ssm:*:*:managed-instance/*",
  "arn:aws:ssm:*:*:association/*"
]
},
{
  "Sid" : "EventRulesManage",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:PutRule",
    "events>DeleteRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/*QuickSetup-*"
  ]
},
{
  "Sid" : "CPacksSLRCreate",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
  ],
  "Condition" : {
    "StringEquals" : {

```

```

        "iam:AWSServiceName" : "config-conforms.amazonaws.com"
    }
}
},
{
    "Sid" : "SSMSLRCreate",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
    }
},
{
    "Sid" : "QSConfigRoleManage",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam>DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
    "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",

```

```
    "arn:aws:iam::*:role/AWSOperationsPack-*"
  ],
},
{
  "Sid" : "QSConfigRolePass",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWS-QuickSetup-*",
    "arn:aws:iam::*:role/AWSOperationsPack-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com",
        "events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DocDescribe",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "LegacyDocClean",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DeleteDocument"
  ],
  "Resource" : "*",
```

```

    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/QuickSetupID" : "*"
      }
    }
  },
  {
    "Sid" : "LegacyIAMClean",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/QuickSetupID" : "*"
      }
    }
  },
  {
    "Sid" : "QSConfigRoleBounded",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteRolePolicy",
      "iam:PutRolePolicy",
      "iam:PutRolePermissionsBoundary"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PermissionsBoundary" : [
          "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
          "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
          "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
          "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
          "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
          "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
        ]
      }
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}

```

```

    },
    "Resource" : [
      "arn:aws:iam::*:role/AWS-QuickSetup-*",
      "arn:aws:iam::*:role/AWSOperationsPack-*"
    ]
  },
  {
    "Sid" : "QSConfigRoleManagedPolicies",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:DetachRolePolicy"
    ],
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : [
          "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
          "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy"
        ]
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "cloudformation.amazonaws.com"
        ]
      }
    },
    "Resource" : [
      "arn:aws:iam::*:role/AWS-QuickSetup-*",
      "arn:aws:iam::*:role/AWSOperationsPack-*"
    ]
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupDevOpsGuruPermissionsBoundary

Description: The AWSQuickSetupDevOpsGuruPermissionsBoundary policy defines the list of permissions that are permitted in an IAM role created by Quick Setup. Quick Setup uses a role created with this policy to enable and configure Amazon DevOps Guru. This policy also provides permissions to enable Systems Manager Explorer.

AWSQuickSetupDevOpsGuruPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupDevOpsGuruPermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:44 UTC
- **Edited time:** June 26, 2024, 09:44 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CreateDevOpsGuruSLRPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "devops-guru.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudformationReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStacks",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DevOpsGuruNotificationChannelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "devops-guru:AddNotificationChannel"
    ],
    "Resource" : [
      "arn:aws:sns::*:DevOpsGuru-Default-Topic",
```

```
    "arn:aws:devops-guru:*:*:/channels"
  ]
},
{
  "Sid" : "DevOpsGuruConfigurationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "devops-guru:UpdateResourceCollection",
    "devops-guru:UpdateServiceIntegration"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:AddPermission",
    "sns:CreateTopic",
    "sns:GetTopicAttributes",
    "sns:Publish",
    "sns:SetTopicAttributes",
    "sns:RemovePermission"
  ],
  "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
},
{
  "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "config:DescribeConfigurationRecorders",
    "compute-optimizer:GetEnrollmentStatus",
    "support:DescribeTrustedAdvisorChecks"
  ],
  "Resource" : "*"
},
}
```

```
{
  "Sid" : "SSMExplorerServiceSettingsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:UpdateServiceSetting",
    "ssm:GetServiceSetting"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupDistributorPermissionsBoundary

Description: QuickSetup creates IAM roles which enable it to configure the Systems Manager Distributor feature on your behalf, and uses this policy when creating such roles to define the boundary of their permissions.

AWSQuickSetupDistributorPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupDistributorPermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:50 UTC
- **Edited time:** June 26, 2024, 09:50 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
```

```

    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "DefaultInstanceRoleManagePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam:UpdateRole",
      "iam:GetRole"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:PrincipalTag/QuickSetupManagerID" : "*"
      },
      "ArnLike" : {
        "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
      }
    },
    "Resource" : [
      "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ]
  },
  {
    "Sid" : "DefaultInstanceRolePassToEC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid" : "DefaultInstanceRolePassToSSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ssm.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "InstanceManagementPoliciesAttachPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:DetachRolePolicy"
    ],
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : [
          "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
          "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
        ]
      },
      "StringLike" : {
        "aws:PrincipalTag/QuickSetupManagerID" : "*"
      },
      "ArnLike" : {
        "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
      }
    }
  },
  {
    "Resource" : "arn:aws:iam::*:role/*"
  },
  {

```

```
    "Sid" : "CreateSystemsManagerSLRPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DefaultInstanceRoleAddPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "IAMReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetInstanceProfile",
      "iam:GetRolePolicy",
      "iam:ListInstanceProfilesForRole",
      "iam:ListRoles"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DefaultInstanceProfileCreatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile"
    ],
  },
```



```

    "Resource" : [
      "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
    ]
  },
  {
    "Sid" : "DefaultInstanceProfileAssociationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateIamInstanceProfile"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:InstanceProfile" : "true"
      },
      "ArnLike" : {
        "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
      }
    }
  },
  {
    "Sid" : "DefaultInstanceProfileDisassociationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
      }
    }
  },
  {
    "Sid" : "ConfigurationAutomationsStartPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm::*:automation-definition/AWSQuickSetup-Distributor-*",
      "arn:aws:ssm::*:automation-definition/UpdateCloudWatchDocument-Distributor-*",

```

```

    "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
    "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
  ]
},
{
  "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListTagsForResource",
    "ssm:GetAutomationExecution",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DescribeInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigurationRecorders",
    "compute-optimizer:GetEnrollmentStatus",
    "support:DescribeTrustedAdvisorChecks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMExplorerServiceSettingsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:UpdateServiceSetting",
    "ssm:GetServiceSetting"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
  ]
}
]

```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupPatchPolicyBaselineAccess

Description: Provides read-only permissions to access patch baselines that have been configured by an administrator in the current AWS account or organization using Quick Setup.

AWSQuickSetupPatchPolicyBaselineAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupPatchPolicyBaselineAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:38 UTC
- **Edited time:** June 26, 2024, 09:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Description: Provides permissions that allow Quick Setup to create resources associated with a patch policy configuration.

AWSQuickSetupPatchPolicyDeploymentRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupPatchPolicyDeploymentRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:57 UTC
- **Edited time:** June 26, 2024, 09:57 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ]
    }
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "CfnManage",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation:UpdateStack",
      "cloudformation>DeleteStack",
      "cloudformation:CreateChangeSet",
      "cloudformation>DeleteChangeSet",
      "cloudformation:ExecuteChangeSet",
      "cloudformation:DescribeChangeSet",
      "cloudformation:DescribeStackResourceDrifts",
      "cloudformation:DetectStackDrift",
      "cloudformation:DetectStackResourceDrift"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
    ]
  },
  {
    "Sid" : "RGroupsGet",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:GetGroupQuery"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "S3BucketsList",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
```

```
"Sid" : "AccessLogsBucketManage",
"Effect" : "Allow",
"Action" : [
  "s3:CreateBucket",
  "s3>DeleteBucket",
  "s3>DeleteBucketPolicy",
  "s3:Put*",
  "s3:Get*",
  "s3:List*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "cloudformation.amazonaws.com"
    ]
  },
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
},
"Resource" : [
  "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
]
},
{
  "Sid" : "LambdaManage",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:UpdateFunction*",
    "lambda:GetFunction",
    "lambda:ListTags",
    "lambda:TagResource",
    "lambda>DeleteFunction",
    "lambda:InvokeFunction",
    "lambda:UntagResource"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  },
  "StringEquals" : {
```

```
    "aws:ResourceAccount" : [
      "${aws:PrincipalAccount}"
    ]
  },
  "Resource" : [
    "arn:aws:lambda:*:*:function:baseline-overrides-*",
    "arn:aws:lambda:*:*:function:delete-name-tags-*"
  ],
  {
    "Sid" : "LogGroupsDescribe",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LogGroupsManage",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:TagResource",
      "logs:PutRetentionPolicy",
      "logs>DeleteLogGroup",
      "logs>ListTagsForResource",
      "logs:UntagResource"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "cloudformation.amazonaws.com"
        ]
      }
    },
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
      "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
    ]
  },
  {
    "Sid" : "QSDocsManage",
    "Effect" : "Allow",
```



```

    "Action" : [
      "ssm:CreateDocument",
      "ssm:UpdateDocument",
      "ssm:DescribeDocument",
      "ssm:UpdateDocumentDefaultVersion",
      "ssm>DeleteDocument",
      "ssm:AddTagsToResource",
      "ssm:RemoveTagsFromResource",
      "ssm:ListTagsForResource"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "cloudformation.amazonaws.com"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
      "arn:aws:ssm:*:*:document/QuickSetup-*"
    ]
  },
  {
    "Sid" : "QSDocsGet",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
      "arn:aws:ssm:*:*:document/QuickSetup-*",
      "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
      "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline"
    ]
  },
  {
    "Sid" : "QSAssociationsManage",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateAssociation",
      "ssm:UpdateAssociation",
      "ssm>DeleteAssociation",
      "ssm:DescribeAssociation"
    ]
  },

```

```

    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "cloudformation.amazonaws.com"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
      "arn:aws:ssm:*:*:document/QuickSetup-*",
      "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
      "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ssm:*:*:managed-instance/*",
      "arn:aws:ssm:*:*:association*"
    ]
  },
  {
    "Sid" : "SSMSLRCreate",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConfigRoleManage",
    "Effect" : "Allow",
    "Action" : [
      "iam:TagRole",
      "iam:UntagRole",
      "iam:GetRole",
      "iam:UpdateRole",
      "iam>DeleteRole",
      "iam:GetRolePolicy",
      "iam>ListAttachedRolePolicies",

```

```
    "iam:ListRolePolicies",
    "iam:ListRoleTags"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  },
  "Resource" : [
    "arn:aws:iam::*:role/AWS-QuickSetup-*"
  ]
},
{
  "Sid" : "ConfigRolePassToSSM",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWS-QuickSetup-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ConfigRolePassToLambda",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWS-QuickSetup-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Sid" : "DocDescribe",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LegacyDocClean",
  "Effect" : "Allow",
  "Action" : [
    "ssm>DeleteDocument"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/QuickSetupID" : "*"
    }
  }
},
{
  "Sid" : "LegacyIAMClean",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteRole",
    "iam>DeleteRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/QuickSetupID" : "*"
    }
  }
},
{
  "Sid" : "ConfigRoleBoundedManage",
  "Effect" : "Allow",
  "Action" : [
    "iam>CreateRole",
```

```
    "iam:AttachRolePolicy",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePolicy",
    "iam:PutRolePermissionsBoundary"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  },
  "Resource" : [
    "arn:aws:iam::*:role/AWS-QuickSetup-*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupPatchPolicyPermissionsBoundary

Description: QuickSetup creates IAM roles which enable it to configure the Systems Manager Patch Manager feature on your behalf, and uses this policy when creating such roles to define the boundary of their permissions.

AWSQuickSetupPatchPolicyPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach `AWSQuickSetupPatchPolicyPermissionsBoundary` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:46 UTC
- **Edited time:** June 26, 2024, 09:46 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "ssm.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "DefaultInstanceRolePermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
            "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
    },
    "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ]
},
{
    "Sid" : "DefaultInstanceRolePassPermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ],
    "Condition" : {
        "StringEquals" : {

```

```

        "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
        ]
    }
},
{
    "Sid" : "PoliciesAttachPermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Condition" : {
        "ArnEquals" : {
            "iam:PolicyARN" : [
                "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
                "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
            ]
        },
        "StringLike" : {
            "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
            "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
    },
    "Resource" : "arn:aws:iam::*:role/*"
},
{
    "Sid" : "CreateSLRPermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
    }
}

```



```
    }
  },
  {
    "Sid" : "InstanceRoleAddPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "ManagedInstanceRoleUpdatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:UpdateManagedInstanceRole"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetInstanceProfile",
      "iam:GetRolePolicy",
      "iam:ListInstanceProfilesForRole",
      "iam:ListRoles"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "InstanceProfileCreatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
    ]
  },
  {

```

```

    "Sid" : "InstanceProfileAssociationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateIamInstanceProfile"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:InstanceProfile" : "true"
      },
      "ArnLike" : {
        "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
      }
    }
  },
  {
    "Sid" : "InstanceProfileDisassociationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
      }
    }
  },
  {
    "Sid" : "SSMAssociationsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeAssociationExecutions",
      "ssm:UpdateAssociation",
      "ssm:DescribeAssociation"
    ],
    "Resource" : [
      "arn:aws:ssm::*:document/AWSQuickSetup-*",
      "arn:aws:ec2::*:instance/*",
      "arn:aws:ssm::*:managed-instance/*",
      "arn:aws:ssm::*:association*"
    ]
  }
]

```

```
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
    "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
  ]
},
{
  "Sid" : "SSMTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource",
    "ssm:RemoveTagsFromResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "QSConfigName-*"
    }
  }
},
{
  "Sid" : "EC2TaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "QSConfigName-*"
    }
  }
},
{
  "Sid" : "RoleTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:TagRole",
    "iam:UntagRole"
  ],
  "Resource" : "*",
```

```

    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : "QSConfigId-*"
      }
    }
  },
  {
    "Sid" : "PatchingReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetPatchBaseline",
      "ssm:GetInventory",
      "ssm:DescribeInstanceInformation",
      "ssm:DescribeAssociation",
      "ssm:GetAutomationExecution",
      "ssm:ListTagsForResource",
      "ec2:DescribeIamInstanceProfileAssociations",
      "ec2:DescribeInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PatchingAutomationsStartPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
      "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
      "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
      "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
      "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*"
    ]
  },
  {
    "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles",
      "config:DescribeConfigurationRecorders",
      "compute-optimizer:GetEnrollmentStatus",
      "support:DescribeTrustedAdvisorChecks"
    ]
  },

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ExplorerServiceSettingsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:UpdateServiceSetting",
      "ssm:GetServiceSetting"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupSchedulerPermissionsBoundary

Description: The AWSQuickSetupSchedulerPermissionsBoundary policy defines the list of permissions that are permitted in an IAM role created by Quick Setup. Quick Setup uses a role created with this policy to enable and configure scheduled operations on Amazon EC2 instances and other resources.

AWSQuickSetupSchedulerPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach `AWSQuickSetupSchedulerPermissionsBoundary` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:53 UTC
- **Edited time:** June 26, 2024, 09:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ssm.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetCalendarState"
    ],
    "Resource" : [
      "arn:aws:ssm::*:document/AWSQuickSetup-ChangeCalendar-*"
    ]
  },
  {
    "Sid" : "EC2ReadOnlyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2StartStopPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances"
    ],
    "Resource" : "arn:aws:ec2::*:instance/*",
    "Condition" : {
      "StringEquals" : {
```



```

        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
},
{
    "Sid" : "AutomationStartPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ssm:StartAutomationExecution"
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
    ]
},
{
    "Sid" : "AssociationsStartOncePermissions",
    "Effect" : "Allow",
    "Action" : [
        "ssm:StartAssociationsOnce"
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:association/*"
    ]
},
{
    "Sid" : "CreateSystemsManagerSLRPermissions",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
    }
},
{
    "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
    "Effect" : "Allow",

```

```
"Action" : [
  "iam:ListRoles",
  "config:DescribeConfigurationRecorders",
  "compute-optimizer:GetEnrollmentStatus",
  "support:DescribeTrustedAdvisorChecks"
],
"Resource" : "*"
},
{
  "Sid" : "SSMExplorerServiceSettingsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:UpdateServiceSetting",
    "ssm:GetServiceSetting"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Description: Quick Setup creates IAM roles which enable it to configure the Host Manager Quick Setup type on your behalf, and uses this policy when creating such roles to define the boundary of their permissions.

AWSQuickSetupSSMHostMgmtPermissionsBoundary is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSetupSSMHostMgmtPermissionsBoundary to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:48 UTC
- **Edited time:** June 26, 2024, 09:48 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

    "Resource" : [
      "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
    ]
  },
  {
    "Sid" : "HostManagementAutomationRolePassPermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ssm.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "DefaultInstanceRoleManagePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam:UpdateRole",
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:PrincipalTag/QuickSetupManagerID" : "*"
      },
      "ArnLike" : {
        "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      }
    }
  },
  {
    "Sid" : "DefaultInstanceRolePassToEC2Permissions",

```

```
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "ec2.amazonaws.com"
    ]
  }
},
{
  "Sid" : "DefaultInstanceRolePassToSSMPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "InstanceManagementPoliciesAttachPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:AttachRolePolicy",
    "iam:DetachRolePolicy"
  ],
  "Condition" : {
    "ArnEquals" : {
      "iam:PolicyARN" : [
        "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
        "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
      ]
    }
  }
}
```

```

    ]
  },
  "StringLike" : {
    "aws:PrincipalTag/QuickSetupManagerID" : "*"
  },
  "ArnLike" : {
    "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
  }
},
"Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "CreateSystemsManagerSLRPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "ssm.amazonaws.com"
    }
  }
},
{
  "Sid" : "DefaultInstanceRoleAddPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "IAMReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile",
    "iam:GetRolePolicy",
    "iam:ListInstanceProfilesForRole",

```

```

    "iam:ListRoles"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DefaultInstanceProfileCreatePermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
  ]
},
{
  "Sid" : "DefaultInstanceProfileAssociationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateIamInstanceProfile"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:InstanceProfile" : "true"
    },
    "ArnLike" : {
      "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
    }
  }
},
{
  "Sid" : "DefaultInstanceProfileDisassociationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
    }
  }
}

```

```

    }
  }
},
{
  "Sid" : "ConfigurationAutomationsStartPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
    "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-CreateAndAttachIAMToInstance-*",
    "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-UpdateExistingInstanceProfile-*",
    "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-InstallAndManageCloudWatchDocument-*",
    "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
    "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
    "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
    "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
    "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
    "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
  ]
},
{
  "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListTagsForResource",
    "ssm:GetAutomationExecution",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DescribeInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigurationRecorders",
    "compute-optimizer:GetEnrollmentStatus",
    "support:DescribeTrustedAdvisorChecks"
  ]
},

```



```
    "Resource" : "*"
  },
  {
    "Sid" : "SSMExplorerServiceSettingsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:UpdateServiceSetting",
      "ssm:GetServiceSetting"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightAssetBundleExportPolicy

Description: Provides the set of permissions required to perform QuickSight Asset Bundle Export Operations

AWSQuickSightAssetBundleExportPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightAssetBundleExportPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 27, 2024, 21:31 UTC
- **Edited time:** March 27, 2024, 21:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightAssetBundleImportPolicy

Description: Provides the set of permissions required to perform QuickSight Asset Bundle Import Operations

AWSQuickSightAssetBundleImportPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightAssetBundleImportPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 27, 2024, 21:40 UTC
- **Edited time:** March 27, 2024, 21:40 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "VPCCConnectionWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:ListVPCCConnections",
    "quicksight:CreateVPCCConnection",
    "quicksight:DescribeVPCCConnection",
    "quicksight>DeleteVPCCConnection",
    "quicksight:UpdateVPCCConnection"
  ],
  "Resource" : "arn:aws:quicksight:*:*:vpccConnection/*"
},
{
  "Sid" : "AssetBundleImportOperations",
```

```
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeAssetBundleImportJob",
      "quicksight:ListAssetBundleImportJobs",
      "quicksight:StartAssetBundleImportJob"
    ],
    "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuicksightAthenaAccess

Description: Quicksight access to Athena API and S3 buckets used for Athena query results

AWSQuicksightAthenaAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSQuicksightAthenaAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** December 09, 2016, 02:31 UTC
- **Edited time:** July 07, 2021, 20:09 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightDescribeRDS

Description: Allow QuickSight to describe the RDS resources

AWSQuickSightDescribeRDS is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightDescribeRDS to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 10, 2015, 23:24 UTC
- **Edited time:** November 10, 2015, 23:24 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightDescribeRedshift

Description: Allow QuickSight to describe Redshift resources

AWSQuickSightDescribeRedshift is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightDescribeRedshift to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 10, 2015, 23:25 UTC
- **Edited time:** November 10, 2015, 23:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightElasticsearchPolicy

Description: Provides access to Amazon Elasticsearch resources from Amazon QuickSight

AWSQuickSightElasticsearchPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightElasticsearchPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 09, 2020, 17:27 UTC
- **Edited time:** September 07, 2021, 23:25 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightIoTAnalyticsAccess

Description: Give QuickSight read-only access to IoT Analytics datasets

AWSQuickSightIoTAnalyticsAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightIoTAnalyticsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 17:00 UTC
- **Edited time:** November 29, 2017, 17:00 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightListIAM

Description: Allow QuickSight to list IAM entities

AWSQuickSightListIAM is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightListIAM to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 10, 2015, 23:25 UTC
- **Edited time:** November 10, 2015, 23:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iam:List*"
  ],
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuicksightOpenSearchPolicy

Description: Provides access to Amazon OpenSearch resources from Amazon QuickSight

AWSQuicksightOpenSearchPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuicksightOpenSearchPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 07, 2021, 23:26 UTC
- **Edited time:** September 07, 2021, 23:26 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    ]
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightSageMakerPolicy

Description: Provides access to Amazon SageMaker resources from Amazon QuickSight

AWSQuickSightSageMakerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightSageMakerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 17, 2020, 17:18 UTC
- **Edited time:** October 30, 2023, 17:57 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3::quicksight-ml.*",
        "arn:aws:s3::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSQuickSightTimestreamPolicy

Description: AWS QuickSight access to AWS Timestream APIs. Customers can attach this policy to AWS QuickSight role to allow retrieval of data and metadata.

AWSQuickSightTimestreamPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSQuickSightTimestreamPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 30, 2020, 21:47 UTC
- **Edited time:** September 30, 2020, 21:47 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSReachabilityAnalyzerServiceRolePolicy

Description: Allows VPC Reachability Analyzer to access AWS resources and integrate with AWS Organizations on your behalf.

AWSReachabilityAnalyzerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 23, 2022, 17:12 UTC
- **Edited time:** May 15, 2024, 20:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
```



```
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnects",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetManagedPrefixListEntries",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListCustomRoutingAccelerators",
"globalaccelerator:ListCustomRoutingEndpointGroups",
"globalaccelerator:ListCustomRoutingListeners",
"globalaccelerator:ListCustomRoutingPortMappings",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeResourcePolicy",
```

```

    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "tag:GetResources",
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ApigatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRefactoringToolkitFullAccess

Description: This policy grants permission to use AWS services with the AWS Toolkit for .NET Refactoring extension for Microsoft Visual Studio. It is intended to be attached to a local AWS profile. The policy allows uploading application artifacts and downloading the resulting artifacts from Amazon S3. It allows building applications into a container image using AWS CodeBuild and storing and retrieving the images from Amazon Elastic Container Registry (Amazon ECR). And it allows deployment of the application to container services on AWS such as Amazon Elastic Container Service (Amazon ECS), optional creation of VPC resources, optional connection to existing infrastructure such as AWS Directory Service, and other related services.

AWSRefactoringToolkitFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSRefactoringToolkitFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 25, 2022, 16:41 UTC
- **Edited time:** March 25, 2024, 18:43 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRefactoringToolkitSidecarPolicy

Description: This policy is intended to be used by Amazon ECS Tasks created for testing applications in AWS using the AWS Toolkit for .NET Refactoring extension for Microsoft Visual Studio. The policy grants access to download application artifacts from Amazon S3, communicate the status of the Task using AWS Systems Manager, and other required services.

AWSRefactoringToolkitSidecarPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSRefactoringToolkitSidecarPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 25, 2022, 16:41 UTC
- **Edited time:** October 29, 2022, 22:15 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    }  
  }  
]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSrePostPrivateCloudWatchAccess

Description: Provides re:Post Private access to publish CloudWatch metrics data

AWSrePostPrivateCloudWatchAccess is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 15, 2023, 16:37 UTC
- **Edited time:** November 15, 2023, 16:37 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRepostSpaceSupportOperationsPolicy

Description: This policy allows the re:Post Space service to create, manage, and resolve Support cases that are created through the Space application.

AWSRepostSpaceSupportOperationsPolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSRepostSpaceSupportOperationsPolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 26, 2023, 21:52 UTC
- **Edited time:** November 26, 2023, 21:52 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResilienceHubAssessmentExecutionPolicy

Description: Policy for AWS Resilience Hub service role which allows access to other AWS services in order to execute assessment.

AWSResilienceHubAssessmentExecutionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSResilienceHubAssessmentExecutionPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2023, 12:32 UTC
- **Edited time:** March 24, 2024, 18:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceAccessManagerFullAccess

Description: Provides full access to AWS Resource Access Manager

AWSResourceAccessManagerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceAccessManagerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 04, 2019, 17:28 UTC
- **Edited time:** June 04, 2019, 17:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
{
  "Action" : [
    "ram:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceAccessManagerReadOnlyAccess

Description: Provides read only access to AWS Resource Access Manager.

AWSResourceAccessManagerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceAccessManagerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 09, 2019, 20:58 UTC
- **Edited time:** December 09, 2019, 20:58 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceAccessManagerResourceShareParticipantAccess

Description: Provides access to AWS Resource Access Manager APIs needed by a resource share participant.

AWSResourceAccessManagerResourceShareParticipantAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceAccessManagerResourceShareParticipantAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 09, 2019, 20:41 UTC
- **Edited time:** December 09, 2019, 20:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceAccessManagerServiceRolePolicy

Description: Policy containing Read-only AWS Resource Access Manager access to customers' Organizations structure. It also contains IAM permissions to self-delete the role.

AWSResourceAccessManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 14, 2018, 19:28 UTC
- **Edited time:** November 14, 2018, 19:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceExplorerFullAccess

Description: This policy grants administrative permissions to access Resource Explorer resources and grants read-only permissions to other AWS services to support this access.

AWSResourceExplorerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceExplorerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 07, 2022, 20:01 UTC
- **Edited time:** November 14, 2023, 16:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceExplorerOrganizationsAccess

Description: This policy grants administrative permissions to Resource Explorer and grants read-only permissions to other AWS services to support this access. The AWS Organizations administrator needs these permissions to setup and manage multi-account search in the console.

AWSResourceExplorerOrganizationsAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceExplorerOrganizationsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 14, 2023, 17:01 UTC
- **Edited time:** November 14, 2023, 17:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceExplorerReadOnlyAccess

Description: This policy grants read-only permissions to search for and view Resource Explorer resources and grants read-only permissions to other AWS services to support this access.

AWSResourceExplorerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceExplorerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 07, 2022, 19:56 UTC
- **Edited time:** November 14, 2023, 16:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceExplorerServiceRolePolicy

Description: Allows Resource Explorer to view resources and CloudTrail events on your behalf to index your resources for search.

AWSResourceExplorerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 25, 2022, 20:35 UTC
- **Edited time:** December 20, 2023, 13:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*:*/restapis",
        "arn:aws:apigateway:*:*/restapis/*/deployments"
      ]
    }
  ]
}
```

```
]
},
{
  "Sid" : "ResourceInventoryAccess",
  "Effect" : "Allow",
  "Action" : [
    "access-analyzer:ListAnalyzers",
    "acm-pca:ListCertificateAuthorities",
    "amplify:ListApps",
    "amplify:ListBackendEnvironments",
    "amplify:ListBranches",
    "amplify:ListDomainAssociations",
    "amplifyuibuilder:ListComponents",
    "amplifyuibuilder:ListThemes",
    "app-integrations:ListEventIntegrations",
    "apprunner:ListServices",
    "apprunner:ListVpcConnectors",
    "appstream:DescribeAppBlocks",
    "appstream:DescribeApplications",
    "appstream:DescribeFleets",
    "appstream:DescribeImageBuilders",
    "appstream:DescribeStacks",
    "appsync:ListGraphQLApis",
    "aps:ListRuleGroupsNamespaces",
    "aps:ListWorkspaces",
    "athena:ListDataCatalogs",
    "athena:ListWorkGroups",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListReportPlans",
    "batch:DescribeComputeEnvironments",
    "batch:DescribeJobQueues",
    "batch:ListSchedulingPolicies",
    "cloudformation:ListStacks",
    "cloudformation:ListStackSets",
    "cloudfront:ListCachePolicies",
    "cloudfront:ListCloudFrontOriginAccessIdentities",
    "cloudfront:ListDistributions",
    "cloudfront:ListFieldLevelEncryptionConfigs",
    "cloudfront:ListFieldLevelEncryptionProfiles",
    "cloudfront:ListFunctions",
    "cloudfront:ListOriginAccessControls",
    "cloudfront:ListOriginRequestPolicies",
    "cloudfront:ListRealtimeLogConfigs",
```



```
"cloudfront:ListResponseHeadersPolicies",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"codeartifact:ListDomains",
"codeartifact:ListRepositories",
"codebuild:ListProjects",
"codecommit:ListRepositories",
"codeguru-profiler:ListProfilingGroups",
"codepipeline:ListPipelines",
"codestar-connections:ListConnections",
"cognito-identity:ListIdentityPools",
"cognito-idp:ListUserPools",
"databrew:ListDatasets",
"databrew:ListRecipes",
"databrew:ListRulesets",
"detective:ListGraphs",
"ds:DescribeDirectories",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeCapacityReservationFleets",
"ec2:DescribeCapacityReservations",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeElasticGpus",
"ec2:DescribeExportImageTasks",
"ec2:DescribeExportTasks",
"ec2:DescribeFleets",
"ec2:DescribeFlowLogs",
"ec2:DescribeFpgaImages",
"ec2:DescribeHostReservations",
"ec2:DescribeHosts",
"ec2:DescribeImages",
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstanceEventWindows",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
```

```
"ec2:DescribeIpamPools",
"ec2:DescribeIpams",
"ec2:DescribeIpamScopes",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInsightsAccessScopeAnalyses",
"ec2:DescribeNetworkInsightsAccessScopes",
"ec2:DescribeNetworkInsightsAnalyses",
"ec2:DescribeNetworkInsightsPaths",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeReservedInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeSubnets",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPolicyTables",
"ec2:DescribeTransitGatewayRouteTableAnnouncements",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeVerifiedAccessEndpoints",
"ec2:DescribeVerifiedAccessGroups",
"ec2:DescribeVerifiedAccessInstances",
"ec2:DescribeVerifiedAccessTrustProviders",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
```

```
"ec2:GetSubnetCidrReservations",
"ecr:DescribeRepositories",
"ecr-public:DescribeRepositories",
"ecs:DescribeCapacityProviders",
"ecs:DescribeServices",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:ListServices",
"ecs:ListTaskDefinitions",
"ecs:ListTasks",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeReservedCacheNodes",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"emr-serverless:ListApplications",
"es:ListDomainNames",
"events:ListEventBuses",
"events:ListRules",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"finspace:ListEnvironments",
"firehose:ListDeliveryStreams",
"fis:ListExperimentTemplates",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"frauddetector:GetEntityTypes",
```

```
"frauddetector:GetEventTypes",
"frauddetector:GetLabels",
"frauddetector:GetOutcomes",
"frauddetector:GetVariables",
"gamelift:ListAliases",
"geo:ListPlaceIndexes",
"geo:ListTrackers",
"greengrass:ListComponents",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"glue:GetDatabases",
"glue:GetJobs",
"glue:GetTables",
"glue:GetTriggers",
"greengrass:ListComponentVersions",
"greengrass:ListGroups",
"healthlake:ListFHIRDatastores",
"iam:ListGroups",
"iam:ListInstanceProfiles",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iot:ListJobTemplates",
```

```
"iot:ListAuthorizers",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListSecurityProfiles",
"iot:ListThings",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListGateways",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListWorkspaces",
"kafka:ListConfigurations",
"kms:ListKeys",
"ivs:ListChannels",
"ivs:ListStreamKeys",
"kafka:ListClusters",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisvideo:ListStreams",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lex:ListBots",
"lex:ListBotAliases",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"lookoutmetrics:ListAlerts",
"lookoutvision:ListProjects",
"mediapackage:ListChannels",
"mediapackage:ListOriginEndpoints",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mq:ListBrokers",
"mediatailor:ListPlaybackConfigurations",
```

```
"memorydb:DescribeACLs",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeUsers",
"mobiletargeting:GetApps",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTemplates",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetDevices",
"networkmanager:GetLinks",
"networkmanager:ListAttachments",
"networkmanager:ListCoreNetworks",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:ListAccounts",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListDelegatedAdministrators",
"panorama:ListPackages",
"personalize:ListDatasetGroups",
"personalize:ListDatasets",
"personalize:ListSchemas",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeReservedDBInstances",
"redshift:DescribeClusterParameterGroups",
```

```
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"rekognition:DescribeProjects",
"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" : [
    "*"
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSResourceGroupsReadOnlyAccess

Description: This is the read only policy for AWS Resource Groups

AWSResourceGroupsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSResourceGroupsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 07, 2018, 10:27 UTC

- **Edited time:** February 05, 2019, 17:56 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRoboMaker_FullAccess

Description: Provides full access to AWS RoboMaker via the AWS Management Console and SDK. Also provides select access to related services (e.g., S3, IAM).

AWSRoboMaker_FullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSRoboMaker_FullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 10, 2020, 18:34 UTC
- **Edited time:** September 16, 2021, 21:06 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRoboMakerReadOnlyAccess

Description: Provides read only access to AWS RoboMaker via the AWS Management Console and SDK

AWSRoboMakerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSRoboMakerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 26, 2018, 05:30 UTC
- **Edited time:** August 28, 2020, 23:10 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ]
    }
  ],
}
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRoboMakerServicePolicy

Description: RoboMaker service policy

AWSRoboMakerServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2018, 06:30 UTC
- **Edited time:** November 11, 2021, 22:23 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRoboMakerServiceRolePolicy

Description: RoboMaker service policy

AWSRoboMakerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSRoboMakerServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 26, 2018, 05:33 UTC
- **Edited time:** November 26, 2018, 05:33 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSRolesAnywhereServicePolicy

Description: Allows IAM Roles Anywhere to publish service/usage metrics to CloudWatch and check the status of Private Certificate Authorities on your behalf.

AWSRolesAnywhereServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 05, 2022, 15:26 UTC
- **Edited time:** July 05, 2022, 15:26 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSS3OnOutpostsServiceRolePolicy

Description: Allow Amazon S3 on Outposts service to manage EC2 network resources on your behalf.

AWSS3OnOutpostsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 03, 2023, 20:32 UTC
- **Edited time:** October 03, 2023, 20:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSavingsPlansFullAccess

Description: Provides full access to Savings Plans service

AWSSavingsPlansFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSavingsPlansFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 06, 2019, 22:45 UTC
- **Edited time:** November 06, 2019, 22:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSavingsPlansReadOnlyAccess

Description: Provides read only access to Savings Plans service

AWSSavingsPlansReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSavingsPlansReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 06, 2019, 22:45 UTC
- **Edited time:** November 06, 2019, 22:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSecurityHubFullAccess

Description: Provides full access to use AWS Security Hub.

AWSecurityHubFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSecurityHubFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 23:54 UTC
- **Edited time:** April 23, 2024, 18:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSecurityHubFullAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSecurityHubOrganizationsAccess

Description: Grants permission to enable and manage AWS Security Hub within an organization. Includes enabling the service across the organization, and determining the delegated administrator account for the service.

AWSecurityHubOrganizationsAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSecurityHubOrganizationsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 15, 2021, 20:53 UTC
- **Edited time:** November 16, 2023, 21:13 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSecurityHubReadOnlyAccess

Description: Provides read only access to AWS Security Hub resources

AWSecurityHubReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSecurityHubReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 28, 2018, 01:34 UTC
- **Edited time:** February 22, 2024, 23:45 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSecurityHubReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",

```

```
        "securityhub:BatchGet*",
        "securityhub:Describe*"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSecurityHubServiceRolePolicy

Description: A service-linked role required for AWS Security Hub to access your resources.

AWSSecurityHubServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 27, 2018, 23:47 UTC
- **Edited time:** November 27, 2023, 03:46 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy

Policy version

Policy version: v14 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogAdminFullAccess

Description: Provides full access to service catalog admin capabilities

AWSServiceCatalogAdminFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSServiceCatalogAdminFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 15, 2018, 17:19 UTC
- **Edited time:** April 13, 2023, 18:43 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogAdminReadOnlyAccess

Description: Provides read-only access to Service Catalog admin capabilities

AWSServiceCatalogAdminReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSServiceCatalogAdminReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 25, 2019, 18:53 UTC
- **Edited time:** October 25, 2019, 18:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogAppRegistryFullAccess

Description: Provides full access to Service Catalog App Registry capabilities

AWSServiceCatalogAppRegistryFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSManagedPolicyAppRegistryFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 12, 2020, 22:25 UTC
- **Edited time:** December 07, 2023, 21:50 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSManagedPolicyAppRegistryFullAccess`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

Description: Provides read-only access to Service Catalog App Registry capabilities

AWSServiceCatalogAppRegistryReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSServiceCatalogAppRegistryReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 12, 2020, 22:34 UTC
- **Edited time:** November 17, 2022, 18:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

Description: Allows Service Catalog AppRegistry to manage Resource Groups on your behalf

AWSServiceCatalogAppRegistryServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 18, 2021, 22:18 UTC
- **Edited time:** October 26, 2022, 16:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogEndUserFullAccess

Description: Provides full access to service catalog enduser capabilities

AWSServiceCatalogEndUserFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSServiceCatalogEndUserFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 15, 2018, 17:22 UTC
- **Edited time:** July 10, 2019, 20:30 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
      ]
    }
  ],
  "Resource" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances"
      ],
      "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"
    }
  }
}
]
```



```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogEndUserReadOnlyAccess

Description: Provides read-only access to Service Catalog end-user capabilities

AWSServiceCatalogEndUserReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSServiceCatalogEndUserReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 25, 2019, 18:49 UTC
- **Edited time:** October 25, 2019, 18:49 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Description: A Service Linked Role Policy for AWS ServiceCatalog to sync with AWS Organizations organization structure

AWSServiceCatalogOrgsDataSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 10, 2023, 20:48 UTC
- **Edited time:** April 10, 2023, 20:48 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceCatalogSyncServiceRolePolicy

Description: A Service Linked Role for AWS ServiceCatalog to sync Provisioning Artifacts from source repositories

AWSServiceCatalogSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 15, 2022, 21:20 UTC
- **Edited time:** May 03, 2024, 17:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForAmazonEKSNodegroup

Description: Permissions required for managing nodegroups in the customer's account. These policies related to management of the following resources: AutoscalingGroups, SecurityGroups, LaunchTemplates and InstanceProfiles.

AWSServiceRoleForAmazonEKSNodegroup is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 07, 2019, 01:34 UTC
- **Edited time:** June 27, 2024, 21:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
```

```

    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DescribeInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks" : "*"
    }
  }
},
{
  "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DescribeInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks:nodegroup-name" : "*"
    }
  }
},
{
  "Sid" : "LaunchTemplateRelatedPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteLaunchTemplate",
    "ec2>CreateLaunchTemplateVersion"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks:nodegroup-name" : "*"
    }
  }
}

```



```
  },
  {
    "Sid" : "AutoscalingRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:CompleteLifecycleAction",
      "autoscaling:PutLifecycleHook",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:EnableMetricsCollection",
      "autoscaling:PutScheduledUpdateGroupAction"
    ],
    "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
  },
  {
    "Sid" : "AllowAutoscalingToCreateSLR",
    "Effect" : "Allow",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    },
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowASGCreationByEKS",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateOrUpdateTags",
      "autoscaling:CreateAutoScalingGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "eks",
          "eks:cluster-name",
          "eks:nodegroup-name"
        ]
      }
    }
  }
}
```

```
},
{
  "Sid" : "AllowPassRoleToAutoscaling",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowPassRoleToEC2",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "PermissionsToManageResourcesForNodegroups",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "ec2:CreateLaunchTemplate",
    "ec2:DescribeInstances",
    "iam:GetInstanceProfile",
    "ec2:DescribeLaunchTemplates",
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:CreateSecurityGroup",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:RunInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:GetConsoleOutput",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSubnets",
    "ec2:DescribeCapacityReservations"
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
  },
  {
    "Sid" : "PermissionsToManageEKSAndKubernetesTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "eks",
          "eks:cluster-name",
          "eks:nodegroup-name",
          "kubernetes.io/cluster/*"
        ]
      }
    }
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForAmazonQDeveloper

Description: This Service Linked Role provides Amazon Q Developer ability to provide usage information.

AWSServiceRoleForAmazonQDeveloper is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 25, 2024, 07:40 UTC
- **Edited time:** April 25, 2024, 07:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
```

```
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Q"
      ]
    }
  }
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedPolicyForCloudWatchAlarmsActionSSMServiceRolePolicy

Description: Provides access to Systems Manager resources used by CloudWatch Alarms

AWSManagedPolicyForCloudWatchAlarmsActionSSMServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 01, 2020, 09:49 UTC
- **Edited time:** October 01, 2020, 09:49 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSManagedPolicyForCloudWatchAlarmsActionSSMServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSManagedPolicyForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

Description: Allows CloudWatch to access RDS Performance Insights metrics on your behalf

AWSManagedPolicyForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 07, 2023, 09:32 UTC
- **Edited time:** September 07, 2023, 09:32 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForCodeGuru-Profiler

Description: A service-linked role required for Amazon CodeGuru Profiler to send notifications on your behalf.

AWSServiceRoleForCodeGuru-Profiler is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 26, 2020, 22:04 UTC
- **Edited time:** June 26, 2020, 22:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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



```
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForCodeWhispererPolicy

Description: This role grants permissions to CodeWhisperer to access data in your account to calculate billing, provides access to create and access security reports in Amazon CodeGuru, and emit data to CloudWatch.

AWSServiceRoleForCodeWhispererPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 24, 2023, 19:39 UTC
- **Edited time:** March 29, 2024, 22:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForEC2ScheduledInstances

Description: Allows EC2 Scheduled Instances to launch and manage spot instances.

AWSServiceRoleForEC2ScheduledInstances is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 12, 2017, 18:31 UTC
- **Edited time:** October 12, 2017, 18:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Description: AWS GroundStation uses this service-linked role to invoke EC2 to find public IPv4 addresses

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 13, 2022, 23:52 UTC
- **Edited time:** December 13, 2022, 23:52 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForImageBuilder

Description: Allows EC2ImageBuilder to call AWS services on your behalf.

AWSServiceRoleForImageBuilder is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2019, 22:02 UTC
- **Edited time:** October 19, 2023, 21:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Policy version

Policy version: v19 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForIoTSiteWise

Description: Allows AWS IoT SiteWise to provision and manage gateways as well as query data. The policy includes required AWS Greengrass permissions for deploying to groups, AWS Lambda permissions for creating and updating service-prefixed functions, and AWS IoT Analytics permissions for querying data from datastores.

AWSServiceRoleForIoTSiteWise is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 14, 2018, 19:19 UTC
- **Edited time:** November 13, 2023, 18:27 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
```

```
"Action" : [
  "iottwinmaker:GetWorkspace",
  "iottwinmaker:ExecuteQuery"
],
"Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "iottwinmaker:linkedServices" : [
      "IOTSITWISE"
    ]
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForLogDeliveryPolicy

Description: Allows Log Delivery service to deliver logs by calling log destination on your behalf.

AWSServiceRoleForLogDeliveryPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 04, 2019, 17:31 UTC
- **Edited time:** July 15, 2021, 20:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForMonitronPolicy

Description: Grants Amazon Monitron permissions to manage AWS resources, including AWS SSO user assignment on your behalf.

AWSServiceRoleForMonitronPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 02, 2020, 19:06 UTC
- **Edited time:** September 29, 2022, 20:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForNeptuneGraphPolicy

Description: Provides Cloudwatch access to publish operational and usage metrics and logs for Amazon Neptune

AWSServiceRoleForNeptuneGraphPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2023, 14:03 UTC
- **Edited time:** November 29, 2023, 14:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Description: Provides permissions to describe and update Private Marketplace resources and describe AWS Organizations

AWSServiceRoleForPrivateMarketplaceAdminPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 14, 2024, 22:28 UTC
- **Edited time:** February 14, 2024, 22:28 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForSMS

Description: Provides access to AWS services and resources necessary to migrate service instances into AWS including EC2, S3 and Cloudformation.

AWSServiceRoleForSMS is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 06, 2019, 18:39 UTC
- **Edited time:** October 15, 2020, 17:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Policy version

Policy version: v10 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRoleForUserSubscriptions

Description: Provides access to the User Subscriptions service to your Identity Center resources to automatically update your subscriptions.

AWSServiceRoleForUserSubscriptions is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 25, 2024, 16:14 UTC
- **Edited time:** April 25, 2024, 16:14 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRolePolicyForBackupReports

Description: Provides AWS Backup permissions to create compliance reports on your behalf

AWSServiceRolePolicyForBackupReports is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 19, 2021, 21:16 UTC
- **Edited time:** March 10, 2023, 00:51 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSServiceRolePolicyForBackupRestoreTesting

Description: This policy contains permissions for testing restores and for cleaning up resources created during tests.

AWSServiceRolePolicyForBackupRestoreTesting is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 10, 2023, 23:37 UTC
- **Edited time:** February 14, 2024, 22:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSShieldDRTAccessPolicy

Description: Provides the AWS DDoS Response Team with limited access to your AWS account to assist with DDoS attack mitigation during a high-severity event.

AWSShieldDRTAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSShieldDRTAccessPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 05, 2018, 22:29 UTC

- **Edited time:** December 15, 2020, 17:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSShieldServiceRolePolicy

Description: Allows AWS Shield to access AWS resources on your behalf to provide DDoS protection.

AWSShieldServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 17, 2021, 19:17 UTC
- **Edited time:** November 17, 2021, 19:17 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSMForSAPServiceLinkedRolePolicy

Description: Provides AWS Systems Manager for SAP with the permissions needed to manage and integrate SAP software with AWS.

AWSSSMForSAPServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 16, 2022, 01:18 UTC
- **Edited time:** April 11, 2024, 18:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSMOpsInsightsServiceRolePolicy

Description: Policy for Service Linked Role AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 16, 2021, 20:12 UTC
- **Edited time:** June 16, 2021, 20:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSODirectoryAdministrator

Description: Administrator access for SSO Directory

AWSSSODirectoryAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AWSSSODirectoryAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 31, 2018, 23:54 UTC
- **Edited time:** October 20, 2022, 20:34 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSODirectoryReadOnly

Description: ReadOnly access for SSO Directory

AWSSSODirectoryReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSSSODirectoryReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 31, 2018, 23:49 UTC
- **Edited time:** November 16, 2022, 18:17 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSOMasterAccountAdministrator

Description: Provides access within AWS SSO to manage AWS Organizations master and member accounts and cloud application

AWSSSOMasterAccountAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AWSSSOMasterAccountAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2018, 20:36 UTC
- **Edited time:** April 26, 2024, 00:38 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSOMemberAccountAdministrator

Description: Provides access within AWS SSO to manage AWS Organizations member accounts and cloud application

AWSSSOMemberAccountAdministrator is an [AWS managed policy](#).

Using this policy

You can attach AWSSSOMemberAccountAdministrator to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2018, 20:45 UTC
- **Edited time:** April 26, 2024, 00:31 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
}  
 ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSOReadOnly

Description: Provides read only access to AWS SSO configurations.

AWSSSOReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSSSOReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2018, 20:24 UTC
- **Edited time:** April 26, 2024, 00:44 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSSOReadOnly

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSSOServiceRolePolicy

Description: Grants AWS SSO permissions to manage AWS resources, including IAM roles, policies and SAML IdP on your behalf.

AWSSSOServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 05, 2017, 18:36 UTC
- **Edited time:** October 20, 2022, 20:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Policy version

Policy version: v17 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",

```

```

    "iam:UpdateRoleDescription",
    "iam:UpdateAssumeRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam>DeleteRolePermissionsBoundary"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "IAMRoleReadActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam>ListRoles"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "IAMRoleCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteRole",
    "iam>DeleteRolePolicy",
    "iam>DetachRolePolicy",
    "iam>ListRolePolicies",
    "iam>ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ]
},
{
  "Sid" : "IAMSLRCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",

```



```
    "iam:GetServiceLinkedRoleDeletionStatus",
    "iam:DeleteRole",
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
  ]
},
{
  "Sid" : "IAMSAMLProviderCreationAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "IAMSAMLProviderUpdateAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:UpdateSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ]
},
{
  "Sid" : "IAMSAMLProviderCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSAMLProvider",
    "iam:GetSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowUnauthAppForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:UnauthorizeApplication"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:DescribeDirectories",
    "ds:DescribeTrusts"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
  "Effect" : "Allow",
  "Action" : [
    "identitystore:DescribeUser",
    "identitystore:DescribeGroup",
    "identitystore:ListGroups",
    "identitystore:ListUsers"
  ],
  "Resource" : [
```

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

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStepFunctionsConsoleFullAccess

Description: An access policy for providing a user/role/etc access to the AWS StepFunctions console. For a full console experience, in addition to this policy, a user may need iam:PassRole permission on other IAM roles that can be assumed by the service.

AWSStepFunctionsConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSStepFunctionsConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 11, 2017, 21:54 UTC
- **Edited time:** January 12, 2017, 00:19 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStepFunctionsFullAccess

Description: An access policy for providing a user/role/etc access to the AWS StepFunctions API. For full access, in addition to this policy, a user MUST have iam:PassRole permission on at least one IAM role that can be assumed by the service.

AWSStepFunctionsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSStepFunctionsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 11, 2017, 21:51 UTC
- **Edited time:** January 11, 2017, 21:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStepFunctionsReadOnlyAccess

Description: An access policy for providing a user/role/etc read only access to the AWS StepFunctions service.

AWSStepFunctionsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSStepFunctionsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 11, 2017, 21:46 UTC
- **Edited time:** April 26, 2024, 18:53 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStorageGatewayFullAccess

Description: Provides full access to AWS Storage Gateway via the AWS Management Console.

AWSStorageGatewayFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSStorageGatewayFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** September 06, 2022, 20:26 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStorageGatewayReadOnlyAccess

Description: Provides access to AWS Storage Gateway via the AWS Management Console.

AWSStorageGatewayReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSStorageGatewayReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** September 06, 2022, 20:24 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSStorageGatewayServiceRolePolicy

Description: Service-linked role used by AWS Storage Gateway to enable integration of other AWS services with Storage Gateway.

AWSStorageGatewayServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 17, 2021, 19:03 UTC
- **Edited time:** February 17, 2021, 19:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

```
    "Resource" : "arn:aws:fsx:*:*:backup/*"  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupplyChainFederationAdminAccess

Description: AWSSupplyChainFederationAdminAccess provides AWS Supply Chain federated users access to the AWS Supply Chain application, including the required permissions to perform actions within the AWS Supply Chain application. The policy provides administrative permissions over IAM Identity Center users and groups and is attached to a role created by AWS Supply Chain on your behalf. You shouldn't attach AWSSupplyChainFederationAdminAccess policy to any other IAM entities.

AWSSupplyChainFederationAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSupplyChainFederationAdminAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 01, 2023, 18:54 UTC
- **Edited time:** November 01, 2023, 18:50 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportAccess

Description: Allows users to access the AWS Support Center.

AWSSupportAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSupportAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSupportAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportAppFullAccess

Description: Provides full access to the AWS Support App and other required services, such as AWS Support and Service Quotas. This policy includes permissions to use the supporting services so that the user can contact AWS Support for support cases, change service quotas, and create the relevant service-linked roles.

AWSSupportAppFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSSupportAppFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 22, 2022, 16:53 UTC
- **Edited time:** August 22, 2022, 16:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportAppReadOnlyAccess

Description: Provides read-only access to the AWS Support App.

AWSSupportAppReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSupportAppReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 22, 2022, 17:01 UTC
- **Edited time:** August 22, 2022, 17:01 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportPlansFullAccess

Description: Provides full access to supportplans.

AWSSupportPlansFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSupportPlansFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 27, 2022, 18:19 UTC
- **Edited time:** May 09, 2023, 21:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportPlansReadOnlyAccess

Description: Provides read-only access to supportplans.

AWSSupportPlansReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSupportPlansReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 27, 2022, 18:08 UTC
- **Edited time:** September 27, 2022, 18:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ]
    }
  ]
}
```



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

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSupportServiceRolePolicy

Description: Allows AWS Support to access AWS resources to provide billing, administrative, and support services.

AWSSupportServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 19, 2018, 18:04 UTC
- **Edited time:** May 02, 2024, 02:47 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

Policy version

Policy version: v36 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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",
"dln:getLifecyclePolicies",
"dln:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
```

```
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
"dms:describeJobLogItems",
"dms:describeJobs",
"dms:describeLaunchConfigurationTemplates",
"dms:describeRecoveryInstances",
"dms:describeRecoverySnapshots",
"dms:describeReplicationConfigurationTemplates",
"dms:describeSourceNetworks",
"dms:describeSourceServers",
"dms:getLaunchConfiguration",
"dms:getReplicationConfiguration",
"dms:listExtensibleSourceServers",
"dms:listLaunchActions",
"dms: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:describeInstanceState",
"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"
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

Description: Grants AWS Systems Manager (SSM) permission to discover AWS account information.

AWSSystemsManagerAccountDiscoveryServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 24, 2019, 17:21 UTC
- **Edited time:** October 17, 2022, 20:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerChangeManagementServicePolicy

Description: Provides access to AWS resources managed or used by the AWS Systems Manager change management framework.

AWSSystemsManagerChangeManagementServicePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 07, 2020, 22:21 UTC
- **Edited time:** December 07, 2020, 22:21 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Description: Provides permissions for AWS Systems Manager Quick Setup to enable and configure AWS Config configuration recording.

AWSSystemsManagerEnableConfigRecordingExecutionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSSystemsManagerEnableConfigRecordingExecutionPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:40 UTC
- **Edited time:** June 26, 2024, 09:40 UTC

- **ARN:** `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig",
        "arn:aws:iam:*:*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig"
      ]
    },
  ],
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "config.amazonaws.com"
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerEnableExplorerExecutionPolicy

Description: This policy grants administrative permissions for enabling Explorer, a capability of AWS Systems Manager. This includes permissions to update related Systems Manager service settings, and to create a service-linked role for Systems Manager.

AWSSystemsManagerEnableExplorerExecutionPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSSystemsManagerEnableExplorerExecutionPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 26, 2024, 09:42 UTC
- **Edited time:** June 26, 2024, 09:42 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "ssm:UpdateServiceSetting",
  "ssm:GetServiceSetting"
],
"Resource" : [
  "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
  "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerForSAPFullAccess

Description: Provides full access to AWS Systems Manager for SAP service

AWSSystemsManagerForSAPFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSystemsManagerForSAPFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2022, 02:11 UTC

- **Edited time:** November 18, 2022, 21:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerForSAPReadOnlyAccess

Description: Provides read only access to AWS Systems Manager for SAP service

AWSSystemsManagerForSAPReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSSystemsManagerForSAPReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 17, 2022, 02:11 UTC
- **Edited time:** November 17, 2022, 02:11 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
```



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:get*",
      "ssm-sap:list*"
    ],
    "Resource" : "arn:*:ssm-sap:*:*:*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Description: IAM role for SSM Explorer to manage OpsData related operations

AWSSystemsManagerOpsDataSyncServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 26, 2021, 20:42 UTC
- **Edited time:** June 28, 2023, 22:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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
    }
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxAssetServerPolicy

Description: This policy grants the AWS Portal Asset Server the necessary permissions required for normal operation.

AWSThinkboxAssetServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxAssetServerPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:18 UTC
- **Edited time:** May 27, 2020, 19:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxAWSPortalAdminPolicy

Description: This policy grants AWS Thinkbox's Deadline software full access to multiple AWS services as required for AWS Portal administration. This includes access to create arbitrary tags on several EC2 resource types.

AWSThinkboxAWSPortalAdminPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxAWSPortalAdminPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:41 UTC

- **Edited time:** April 12, 2024, 20:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
```



```
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeRouteTables",
"ec2:DescribeNatGateways",
"ec2:DescribeTags",
"ec2:DescribeKeyPairs",
"ec2:DescribePlacementGroups",
"ec2:DescribeInstanceTypeOfferings",
"ec2:DescribeRegions",
"ec2:DescribeSpotFleetRequestHistory",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSpotFleetInstances",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotPriceHistory",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeVpcEndpoints",
"ec2:GetConsoleOutput",
"ec2:ImportKeyPair",
"ec2:ReleaseAddress",
"ec2:RequestSpotFleet",
"ec2:CancelSpotFleetRequests",
"ec2:DisassociateAddress",
"ec2>DeleteFleets",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteVpc",
"ec2>DeletePlacementGroup",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteInternetGateway",
"ec2>DeleteSecurityGroup",
"ec2:RevokeSecurityGroupIngress",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2:DisassociateRouteTable",
"ec2>DeleteSubnet",
"ec2>DeleteNatGateway",
"ec2:DetachInternetGateway",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyFleet",
"ec2:ModifySpotFleetRequest",
"ec2:ModifyVpcAttribute"
],
"Resource" : "*"

```

```
},
{
  "Sid" : "AWSThinkboxAWSPortal2",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal3",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:InstanceProfile" : "arn:aws:iam:*:*:instance-profile/AWSPortal*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal4",
  "Effect" : "Allow",
  "Action" : "ec2:TerminateInstances",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal5",
  "Effect" : "Allow",
  "Action" : "ec2:TerminateInstances",
  "Resource" : "*",
```

```
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal6",
    "Effect" : "Allow",
    "Action" : "ec2:TerminateInstances",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal7",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  }
}
```

```
"Sid" : "AWSThinkboxAWSPortal9",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags",
  "ec2:DeleteTags"
],
"Resource" : [
  "arn:aws:ec2:*:*:subnet/*",
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:internet-gateway/*",
  "arn:aws:ec2:*:*:route-table/*",
  "arn:aws:ec2:*:*:volume/*",
  "arn:aws:ec2:*:*:vpc/*",
  "arn:aws:ec2:*:*:natgateway/*",
  "arn:aws:ec2:*:*:elastic-ip/*"
]
},
{
  "Sid" : "AWSThinkboxAWSPortal10",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal11",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:instance-profile/AWSPortal*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal12",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetPolicy",
    "iam:ListEntitiesForPolicy",
    "iam:ListPolicyVersions"
  ],
  "Resource" : [
```

```
    "arn:aws:iam::*:policy/AWSPortal*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal13",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetRolePolicy"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal14",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal15",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
  "Condition" : {
    "StringEquals" : {
```

```

        "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
        ]
    }
},
{
    "Sid" : "AWSThinkboxAWSPortal16",
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3>DeleteBucket",
        "s3>DeleteObject",
        "s3>DeleteBucketPolicy",
        "s3>DeleteObjectVersion"
    ],
    "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal17",
    "Effect" : "Allow",

```

```
"Action" : [
  "s3:PutBucketPolicy"
],
"Resource" : [
  "arn:aws:s3::*:logs-for-aws-portal-cache*"
]
},
{
  "Sid" : "AWSThinkboxAWSPortal18",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketOwnershipControls"
  ],
  "Resource" : [
    "arn:aws:s3::*:logs-for-stack*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal19",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal20",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:Scan"
  ],
  "Resource" : "arn:aws:dynamodb::*:table/DeadlineFleetHealth*"
},
{
  "Sid" : "AWSThinkboxAWSPortal21",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation>DeleteStack",
    "cloudformation>DeleteChangeSet",
    "cloudformation:ListStackResources",
    "cloudformation:CreateChangeSet",
```

```
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:UpdateTerminationProtection",
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/stack*/**",
    "arn:aws:cloudformation:*:*:stack/Deadline*/**"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal22",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:EstimateTemplateCost",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal23",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:PutRetentionPolicy",
    "logs>DeleteRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
},
{
  "Sid" : "AWSThinkboxAWSPortal24",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs>CreateLogGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal25",
  "Effect" : "Allow",
```



```
"Action" : [
  "kms:Encrypt",
  "kms:GenerateDataKey"
],
"Resource" : [
  "*"
],
"Condition" : {
  "StringLike" : {
    "kms:ViaService" : [
      "s3.*.amazonaws.com",
      "secretsmanager.*.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "AWSThinkboxAWSPortal26",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:Name" : [
        "rcs-tls-pw*"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal27",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager>DeleteSecret",
    "secretsmanager:UpdateSecret",
    "secretsmanager:DescribeSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
}
]
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxAWSPortalGatewayPolicy

Description: This policy grants the AWS Portal Gateway machine the necessary permissions required for normal operation.

AWSThinkboxAWSPortalGatewayPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxAWSPortalGatewayPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:05 UTC
- **Edited time:** June 30, 2020, 16:02 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxAWSPortalWorkerPolicy

Description: This policy grants the Deadline Workers in AWS Portal the necessary permissions required for normal operation.

AWSThinkboxAWSPortalWorkerPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxAWSPortalWorkerPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:15 UTC
- **Edited time:** December 07, 2020, 23:27 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Description: Grants permissions required for the operation of AWS Thinkbox's Deadline Resource Tracker. This includes full access to some EC2 actions, including DeleteFleets and CancelSpotFleetRequests.

AWSThinkboxDeadlineResourceTrackerAccessPolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSThinkboxDeadlineResourceTrackerAccessPolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:25 UTC
- **Edited time:** May 27, 2020, 19:25 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Description: Grants permissions required to create, destroy, and administer AWS Thinkbox's Deadline Resource Tracker.

AWSThinkboxDeadlineResourceTrackerAdminPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxDeadlineResourceTrackerAdminPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:29 UTC
- **Edited time:** April 12, 2024, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
  ]
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Description: Grants permissions required for AWS Thinkbox's Deadline Spot Event Plugin. This includes permission to request, modify, and cancel a spot fleet, as well as limited PassRole permission.

AWSThinkboxDeadlineSpotEventPluginAdminPolicy is an [AWS managed policy](#).

Using this policy

You can attach AWSThinkboxDeadlineSpotEventPluginAdminPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:38 UTC
- **Edited time:** May 27, 2020, 19:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Description: Grant permissions required for an EC2 instance running AWS Thinkbox Deadline Spot Event Plugin Worker software.

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy is an [AWS managed policy](#).

Using this policy

You can attach `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 27, 2020, 19:35 UTC
- **Edited time:** December 07, 2020, 23:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
    ]
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTransferConsoleFullAccess

Description: Provides full access to AWS Transfer via the AWS Management Console

AWSTransferConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSTransferConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 14, 2020, 19:33 UTC
- **Edited time:** December 14, 2020, 19:33 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTransferFullAccess

Description: Provides full access to AWS Transfer Service.

AWSTransferFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSTransferFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 14, 2020, 19:37 UTC
- **Edited time:** December 14, 2020, 19:37 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSTransferFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTransferLoggingAccess

Description: Allows AWS Transfer full access to create log streams and groups and put log events to your account

AWSTransferLoggingAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSTransferLoggingAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 14, 2019, 15:32 UTC
- **Edited time:** January 14, 2019, 15:32 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTransferReadOnlyAccess

Description: Provide readonly access to AWS Transfer services.

AWSTransferReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSTransferReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 27, 2020, 17:54 UTC
- **Edited time:** August 27, 2020, 17:54 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTrustedAdvisorPriorityFullAccess

Description: Provides full access to AWS Trusted Advisor Priority. This policy also enables the user to add Trusted Advisor as a trusted service with AWS Organizations and to specify delegated administrator accounts for Trusted Advisor Priority.

AWSTrustedAdvisorPriorityFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSTrustedAdvisorPriorityFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 16, 2022, 16:08 UTC
- **Edited time:** August 16, 2022, 16:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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"
        ]
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

Description: Provides read-only access to AWS Trusted Advisor Priority. This includes permission to view the delegated administrator accounts.

AWSTrustedAdvisorPriorityReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSTrustedAdvisorPriorityReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 16, 2022, 16:35 UTC
- **Edited time:** August 16, 2022, 16:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
            ]
        }
    }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTrustedAdvisorReportingServiceRolePolicy

Description: Service Policy for Trusted Advisor Multi-account Reporting

AWSTrustedAdvisorReportingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 19, 2019, 17:41 UTC
- **Edited time:** February 28, 2023, 23:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSTrustedAdvisorServiceRolePolicy

Description: Access for the AWS Trusted Advisor Service to help reduce cost, increase performance, and improve security of your AWS environment.

AWSTrustedAdvisorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 22, 2018, 21:24 UTC
- **Edited time:** June 11, 2024, 18:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Policy version

Policy version: v13 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSUserNotificationsServiceLinkedRolePolicy

Description: Allows AWS User Notifications to call AWS services on your behalf.

AWSUserNotificationsServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 19, 2023, 13:28 UTC
- **Edited time:** April 19, 2023, 13:28 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVendorInsightsAssessorFullAccess

Description: Provides full access for viewing entitled Vendor Insights resources and managing Vendor Insights subscriptions

AWSVendorInsightsAssessorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSVendorInsightsAssessorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 26, 2022, 15:05 UTC
- **Edited time:** December 01, 2022, 00:51 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVendorInsightsAssessorReadOnly

Description: Provides read-only access for viewing entitled Vendor Insights resources

AWSVendorInsightsAssessorReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSVendorInsightsAssessorReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 26, 2022, 15:05 UTC
- **Edited time:** December 01, 2022, 00:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVendorInsightsVendorFullAccess

Description: Provides full access for creating and managing the Vendor Insights resources

AWSVendorInsightsVendorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSVendorInsightsVendorFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 26, 2022, 15:05 UTC
- **Edited time:** October 19, 2023, 01:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVendorInsightsVendorReadOnly

Description: Provides read-only access for viewing the Vendor Insights resources

AWSVendorInsightsVendorReadOnly is an [AWS managed policy](#).

Using this policy

You can attach AWSVendorInsightsVendorReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 26, 2022, 15:05 UTC
- **Edited time:** December 01, 2022, 00:54 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
    }
  ]
}
```


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVpcLatticeServiceRolePolicy

Description: Allows VPC Lattice to access AWS resources on your behalf.

AWSVpcLatticeServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 30, 2022, 20:47 UTC
- **Edited time:** November 30, 2022, 20:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/VpcLattice"
      }
    }
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVPCS2SVpnServiceRolePolicy

Description: Allow Site-to-Site VPN to create and manage resources related to your VPN Connections.

AWSVPCS2SVpnServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 06, 2019, 14:13 UTC
- **Edited time:** August 06, 2019, 14:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVPCTransitGatewayServiceRolePolicy

Description: Allow VPC Transit Gateway to create and manage necessary resources for your Transit Gateway VPC Attachments.

AWSVPCTransitGatewayServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2018, 16:21 UTC
- **Edited time:** April 15, 2021, 16:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSVPCVerifiedAccessServiceRolePolicy

Description: Policy to enable AWS Verified Access service to provision endpoints on your behalf

AWSVPCVerifiedAccessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2022, 03:35 UTC
- **Edited time:** November 17, 2023, 21:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWAFConsoleFullAccess

Description: Provides full access to AWS WAF via the AWS Management Console. Note that this policy also grants permissions to list and update Amazon CloudFront distributions, permissions to view load balancers on AWS Elastic Load Balancing, permissions to view Amazon API Gateway REST APIs and stages, permissions to list and view Amazon CloudWatch metrics, and permissions to view regions enabled within the account.

AWSWAFConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `AWSWAFConsoleFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 06, 2020, 18:38 UTC
- **Edited time:** June 05, 2023, 20:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWAFConsoleReadOnlyAccess

Description: Provides read-only access to AWS WAF via the AWS Management Console. Note that this policy also grants permissions to list Amazon CloudFront distributions, permissions to view load balancers on AWS Elastic Load Balancing, permissions to view Amazon API Gateway REST APIs and stages, permissions to list and view Amazon CloudWatch metrics, and permissions to view regions enabled within the account.

AWSWAFConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSWAFConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 06, 2020, 18:43 UTC
- **Edited time:** June 05, 2023, 20:56 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWAFFullAccess

Description: Provides full access to AWS WAF actions.

AWSWAFFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSWAFFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 06, 2015, 20:44 UTC
- **Edited time:** June 05, 2023, 20:55 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSWAFFullAccess

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        ]
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWAFReadOnlyAccess

Description: Provides read only access to AWS WAF actions.

AWSWAFReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSWAFReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 06, 2015, 20:43 UTC
- **Edited time:** June 05, 2023, 20:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

Description: Allows WellArchitected to access AWS services and resources that relate to WellArchitected resources on behalf of customers.

AWSWellArchitectedDiscoveryServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 26, 2023, 18:36 UTC
- **Edited time:** April 26, 2023, 18:36 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
```

```

    "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-*"
  ]
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

Description: Allows Well-Architected to access Organizations on your behalf.

AWSWellArchitectedOrganizationsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 23, 2022, 17:15 UTC
- **Edited time:** July 25, 2022, 18:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSWickrFullAccess

Description: This policy grants full administrative permissions to the Wickr service, including the Wickr administrative functions under the AWS Management Console.

AWSWickrFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSWickrFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 20:36 UTC
- **Edited time:** November 27, 2022, 20:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "wickr:*",
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSXrayCrossAccountSharingConfiguration

Description: Provides capabilities to manage Observability Access Manager links and establish sharing of X-Ray traces

AWSXrayCrossAccountSharingConfiguration is an [AWS managed policy](#).

Using this policy

You can attach AWSXrayCrossAccountSharingConfiguration to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 13:46 UTC
- **Edited time:** November 27, 2022, 13:46 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSXRayDaemonWriteAccess

Description: Allow the AWS X-Ray Daemon to relay raw trace segments data to the service's API and retrieve sampling data (rules, targets, etc.) to be used by the X-Ray SDK.

AWSXRayDaemonWriteAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSXRayDaemonWriteAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 28, 2018, 23:00 UTC
- **Edited time:** February 13, 2024, 21:58 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Sid" : "AWSXRayDaemonWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingRules",
      "xray:GetSamplingTargets",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSXrayFullAccess

Description: AWS X-Ray full access managed policy

AWSXrayFullAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSXrayFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2016, 18:30 UTC

- **Edited time:** April 11, 2024, 17:07 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSXrayFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSXrayReadOnlyAccess

Description: AWS X-Ray read only managed policy

AWSXrayReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSXrayReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2016, 18:27 UTC
- **Edited time:** February 14, 2024, 00:35 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
    "*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSXrayWriteOnlyAccess

Description: AWS X-Ray write only managed policy

AWSXrayWriteOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach AWSXrayWriteOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** December 01, 2016, 18:19 UTC
- **Edited time:** August 28, 2018, 23:03 UTC
- **ARN:** arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

Description: Provides administrative access for ARC zonal shift practice runs, and access to CloudWatch alarm statuses to monitor practice runs.

AWSZonalAutoshiftPracticeRunSLRPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2023, 17:34 UTC
- **Edited time:** November 29, 2023, 17:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

BatchServiceRolePolicy

Description: Provides access for the AWS Batch service to manage the required resources, including Amazon EC2 and Amazon ECS resources.

BatchServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 10, 2021, 06:55 UTC
- **Edited time:** December 05, 2023, 22:52 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Billing

Description: Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

Billing is an [AWS managed policy](#).

Using this policy

You can attach Billing to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:33 UTC
- **Edited time:** May 23, 2024, 23:26 UTC
- **ARN:** arn:aws:iam::aws:policy/job-function/Billing

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CertificateManagerServiceRolePolicy

Description: Amazon Certificate Manager Service Role Policy

CertificateManagerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 25, 2020, 17:56 UTC
- **Edited time:** June 25, 2020, 17:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:IssueCertificate",
      "acm-pca:GetCertificate"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ClientVPNServiceConnectionsRolePolicy

Description: Policy to enable AWS Client VPN to manage your Client VPN endpoint connections.

ClientVPNServiceConnectionsRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 12, 2020, 19:48 UTC
- **Edited time:** August 12, 2020, 19:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ClientVPNServiceRolePolicy

Description: Policy to enable AWS Client VPN to manage your Client VPN endpoints.

ClientVPNServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 10, 2018, 21:20 UTC

- **Edited time:** August 12, 2020, 19:39 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

Description: Service Role for CloudFormation StackSets (Organization Master Account)

CloudFormationStackSetsOrgAdminServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 10, 2019, 00:20 UTC
- **Edited time:** December 10, 2019, 00:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

Description: Service Role for CloudFormation StackSets (Organization Member Account)

CloudFormationStackSetsOrgMemberServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 09, 2019, 23:52 UTC
- **Edited time:** December 09, 2019, 23:52 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"  
    }  
  }  
}  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudFrontFullAccess

Description: Provides full access to the CloudFront console plus the ability to list Amazon S3 buckets via the AWS Management Console.

CloudFrontFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudFrontFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** January 04, 2024, 16:56 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudFrontFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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::*:*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudFrontReadOnlyAccess

Description: Provides access to CloudFront distribution configuration information and list distributions via the AWS Management Console.

CloudFrontReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudFrontReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** January 04, 2024, 16:55 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudHSMServiceRolePolicy

Description: Enables access to AWS resources used or managed by CloudHSM

CloudHSMServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 06, 2017, 19:12 UTC
- **Edited time:** November 06, 2017, 19:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:logs:*:*:*"
    ]
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudSearchFullAccess

Description: Provides full access to the Amazon CloudSearch configuration service.

CloudSearchFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudSearchFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** February 06, 2015, 18:39 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudSearchFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudSearchReadOnlyAccess

Description: Provides read only access to the Amazon CloudSearch configuration service.

CloudSearchReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudSearchReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** February 06, 2015, 18:39 UTC

- **ARN:** `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudTrailServiceRolePolicy

Description: Permission policy for CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** October 24, 2018, 21:21 UTC
- **Edited time:** November 27, 2023, 01:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
    }
  }
}
```

```
    }  
  ]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatch-CrossAccountAccess

Description: Allows CloudWatch to assume CloudWatch-CrossAccountSharing roles in remote accounts on behalf of the current account in order to display data cross-account, cross-region

CloudWatch-CrossAccountAccess is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 23, 2019, 09:59 UTC
- **Edited time:** July 23, 2019, 09:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchActionsEC2Access

Description: Provides read-only access to CloudWatch alarms and metrics as well as EC2 metadata. Provides access to Stop, Terminate and Reboot EC2 instances.

CloudWatchActionsEC2Access is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchActionsEC2Access to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 07, 2015, 00:00 UTC
- **Edited time:** July 07, 2015, 00:00 UTC

- **ARN:** `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchAgentAdminPolicy

Description: Full permissions required to use AmazonCloudWatchAgent.

CloudWatchAgentAdminPolicy is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchAgentAdminPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 07, 2018, 00:52 UTC
- **Edited time:** February 05, 2024, 20:59 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchAgentServerPolicy

Description: Permissions required to use AmazonCloudWatchAgent on servers

CloudWatchAgentServerPolicy is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchAgentServerPolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** March 07, 2018, 01:06 UTC
- **Edited time:** February 06, 2024, 16:37 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchApplicationInsightsFullAccess

Description: Provides full access to CloudWatch Application Insights and required dependencies.

CloudWatchApplicationInsightsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchApplicationInsightsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 24, 2020, 18:44 UTC
- **Edited time:** January 25, 2022, 17:51 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchApplicationInsightsReadOnlyAccess

Description: Provides read only access to CloudWatch Application Insights.

CloudWatchApplicationInsightsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchApplicationInsightsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** November 24, 2020, 18:48 UTC
- **Edited time:** November 24, 2020, 18:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Description: Cloudwatch Application Insights Service Linked Role Policy

CloudwatchApplicationInsightsServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 01, 2018, 16:22 UTC
- **Edited time:** May 11, 2023, 16:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Policy version

Policy version: v24 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
        "*"
    ]
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchApplicationSignalsFullAccess

Description: Provide full access to CloudWatch Application Signals service and scoped access to the dependencies needed to use and operate this service.

CloudWatchApplicationSignalsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchApplicationSignalsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 06, 2024, 22:50 UTC
- **Edited time:** June 06, 2024, 22:50 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchApplicationSignalsReadOnlyAccess

Description: Provides read only access to CloudWatch Application Signals service and scoped access to the dependencies needed to use this service

CloudWatchApplicationSignalsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchApplicationSignalsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 06, 2024, 22:48 UTC
- **Edited time:** June 06, 2024, 22:48 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
```

```

    "Action" : [
      "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
      "application-signals:GetService",
      "application-signals:GetServiceLevelObjective",
      "application-signals:ListServiceLevelObjectives",
      "application-signals:ListServiceDependencies",
      "application-signals:ListServiceDependents",
      "application-signals:ListServiceOperations",
      "application-signals:ListServices",
      "application-signals:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs::*:log-group:/aws/application-signals/data:*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:StopQuery",
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "*"
  }

```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchApplicationSignalsServiceRolePolicy

Description: Policy grants permission to CloudWatch Application Signals to collect monitoring and tagging data from other relevant AWS services.

CloudWatchApplicationSignalsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 09, 2023, 18:09 UTC
- **Edited time:** April 26, 2024, 21:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
    }
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchAutomaticDashboardsAccess

Description: Provides access to the non-CloudWatch APIs used to display CloudWatch Automatic Dashboards, including the contents of objects such as Lambda functions

CloudWatchAutomaticDashboardsAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchAutomaticDashboardsAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 23, 2019, 10:01 UTC
- **Edited time:** April 20, 2021, 13:05 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchCrossAccountSharingConfiguration

Description: Provides capabilities to manage Observability Access Manager links and establish sharing of CloudWatch resources

CloudWatchCrossAccountSharingConfiguration is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchCrossAccountSharingConfiguration to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 14:01 UTC
- **Edited time:** November 27, 2022, 14:01 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
      ]
    }
  ]
}
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchEventsBuiltInTargetExecutionAccess

Description: Allows built-in targets in Amazon CloudWatch Events to perform EC2 actions on your behalf.

CloudWatchEventsBuiltInTargetExecutionAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchEventsBuiltInTargetExecutionAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 14, 2016, 18:35 UTC
- **Edited time:** January 14, 2016, 18:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchEventsFullAccess

Description: Provides full access to Amazon CloudWatch Events.

CloudWatchEventsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchEventsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy

- **Creation time:** January 14, 2016, 18:37 UTC
- **Edited time:** December 01, 2022, 17:05 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchEventsInvocationAccess

Description: Allows Amazon CloudWatch Events to relay events to the streams in AWS Kinesis Streams in your account.

CloudWatchEventsInvocationAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchEventsInvocationAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** January 14, 2016, 18:36 UTC
- **Edited time:** January 14, 2016, 18:36 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchEventsReadOnlyAccess

Description: Provides read only access to Amazon CloudWatch Events.

CloudWatchEventsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchEventsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 14, 2016, 18:27 UTC
- **Edited time:** December 01, 2022, 16:29 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchEventsServiceRolePolicy

Description: Allow AWS CloudWatch to execute actions on your behalf configured through alarms and events.

CloudWatchEventsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 17, 2017, 00:42 UTC
- **Edited time:** November 17, 2017, 00:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchFullAccess

Description: Provides full access to CloudWatch.

CloudWatchFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 27, 2022, 13:23 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
    }
  ]
}
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchFullAccessV2

Description: Provides full access to CloudWatch.

CloudWatchFullAccessV2 is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchFullAccessV2 to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 01, 2023, 11:32 UTC
- **Edited time:** May 17, 2024, 22:20 UTC
- **ARN:** `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```

"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/*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchInternetMonitorServiceRolePolicy

Description: Allows Internet Monitor to access EC2, Workspaces, and CloudFront resources, and other required services on your behalf.

CloudWatchInternetMonitorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 27, 2022, 17:46 UTC
- **Edited time:** July 20, 2023, 04:46 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchLambdaInsightsExecutionRolePolicy

Description: Policy required for the Lambda Insights Extension

CloudWatchLambdaInsightsExecutionRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchLambdaInsightsExecutionRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 07, 2020, 19:27 UTC

- **Edited time:** October 07, 2020, 19:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchLogsCrossAccountSharingConfiguration

Description: Provides capabilities to manage Observability Access Manager links and establish sharing of CloudWatch Logs resources

CloudWatchLogsCrossAccountSharingConfiguration is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchLogsCrossAccountSharingConfiguration to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 13:55 UTC
- **Edited time:** November 27, 2022, 13:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchLogsFullAccess

Description: Provides full access to CloudWatch Logs

CloudWatchLogsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchLogsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 26, 2023, 18:12 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchLogsFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchLogsReadOnlyAccess

Description: Provides read only access to CloudWatch Logs

CloudWatchLogsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchLogsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** November 26, 2023, 18:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchNetworkMonitorServiceRolePolicy

Description: Allows CloudWatch Network Monitor to access and manage EC2 and VPC resources, publish data to CloudWatch and access other required services on your behalf.

CloudWatchNetworkMonitorServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 21, 2023, 18:53 UTC
- **Edited time:** December 21, 2023, 18:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchReadOnlyAccess

Description: Provides read only access to CloudWatch.

CloudWatchReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** May 17, 2024, 22:17 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchSyntheticsFullAccess

Description: Provides full access to CloudWatch Synthetics.

CloudWatchSyntheticsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchSyntheticsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 25, 2019, 17:39 UTC
- **Edited time:** May 06, 2022, 18:14 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

Policy version

Policy version: v9 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        ]
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CloudWatchSyntheticsReadOnlyAccess

Description: Provides read only access to CloudWatch Synthetics.

CloudWatchSyntheticsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CloudWatchSyntheticsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 25, 2019, 17:45 UTC
- **Edited time:** March 06, 2020, 19:26 UTC
- **ARN:** arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "synthetics:Describe*",
      "synthetics:Get*",
      "synthetics:List*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComprehendDataAccessRolePolicy

Description: Policy for AWS Comprehend service role which allows access to S3 resources for data access

ComprehendDataAccessRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach ComprehendDataAccessRolePolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** March 06, 2019, 22:28 UTC
- **Edited time:** March 06, 2019, 22:28 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*Comprehend*",
      "arn:aws:s3::*comprehend*"
    ]
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComprehendFullAccess

Description: Provides full access to Amazon Comprehend.

ComprehendFullAccess is an [AWS managed policy](#).

Using this policy

You can attach `ComprehendFullAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 18:08 UTC
- **Edited time:** December 05, 2017, 01:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/ComprehendFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComprehendMedicalFullAccess

Description: Provides full access to Amazon Comprehend Medical

ComprehendMedicalFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ComprehendMedicalFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 17:55 UTC
- **Edited time:** November 27, 2018, 17:55 UTC
- **ARN:** `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
{
  "Action" : [
    "comprehendmedical:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComprehendReadOnly

Description: Provides read-only access to Amazon Comprehend.

ComprehendReadOnly is an [AWS managed policy](#).

Using this policy

You can attach ComprehendReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 18:10 UTC
- **Edited time:** April 26, 2022, 21:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/ComprehendReadOnly`

Policy version

Policy version: v11 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComputeOptimizerReadOnlyAccess

Description: Provides read only access to ComputeOptimizer.

ComputeOptimizerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach ComputeOptimizerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 07, 2020, 00:11 UTC
- **Edited time:** June 20, 2024, 16:15 UTC
- **ARN:** arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",

```

```
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters"
  ],
  "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ComputeOptimizerServiceRolePolicy

Description: Allows ComputeOptimizer to call AWS services and collect workload details on your behalf.

ComputeOptimizerServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 03, 2019, 08:45 UTC
- **Edited time:** June 13, 2022, 19:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ConfigConformsServiceRolePolicy

Description: Policy needed for AWSConfig to create conformance packs

ConfigConformsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 25, 2019, 21:38 UTC

- **Edited time:** January 12, 2023, 04:17 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
```

```
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CostOptimizationHubAdminAccess

Description: This managed policy provides admin access to Cost Optimization Hub.

CostOptimizationHubAdminAccess is an [AWS managed policy](#).

Using this policy

You can attach CostOptimizationHubAdminAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 19, 2023, 00:03 UTC
- **Edited time:** December 19, 2023, 00:03 UTC
- **ARN:** arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}

```

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CostOptimizationHubReadOnlyAccess

Description: This managed policy provides read-only access to Cost Optimization Hub.

CostOptimizationHubReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach CostOptimizationHubReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 13, 2023, 18:04 UTC
- **Edited time:** December 13, 2023, 18:04 UTC
- **ARN:** arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CostOptimizationHubServiceRolePolicy

Description: Allows Cost Optimization Hub to retrieve organization information and collect optimization-related data and metadata.

CostOptimizationHubServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 26, 2023, 08:03 UTC
- **Edited time:** November 26, 2023, 08:03 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
        "*"
    ]
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

CustomerProfilesServiceLinkedRolePolicy

Description: Allows Amazon Connect Customer Profiles to access AWS services and resources on your behalf.

CustomerProfilesServiceLinkedRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 07, 2023, 22:56 UTC
- **Edited time:** March 07, 2023, 22:56 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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_*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DatabaseAdministrator

Description: Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

DatabaseAdministrator is an [AWS managed policy](#).

Using this policy

You can attach DatabaseAdministrator to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:25 UTC
- **Edited time:** January 08, 2019, 00:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DataScientist

Description: Grants permissions to AWS data analytics services.

DataScientist is an [AWS managed policy](#).

Using this policy

You can attach DataScientist to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:28 UTC
- **Edited time:** December 03, 2019, 16:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/job-function/DataScientist`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        ]
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DAXServiceRolePolicy

Description: This policy allows DAX to create and manage Network interface, Security group, Subnet and Vpc on behalf of customer

DAXServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 05, 2018, 17:51 UTC
- **Edited time:** March 05, 2018, 17:51 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Description: Permissions required to support Amazon CloudWatch Contributor Insights for Amazon DynamoDB.

DynamoDBCloudWatchContributorInsightsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 15, 2019, 21:13 UTC
- **Edited time:** November 15, 2019, 21:13 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DynamoDBKinesisReplicationServiceRolePolicy

Description: Provide AWS DynamoDB access to KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 12, 2020, 00:43 UTC
- **Edited time:** November 12, 2020, 00:43 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

DynamoDBReplicationServiceRolePolicy

Description: Permissions required by DynamoDB for cross-region data replication

DynamoDBReplicationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 09, 2017, 23:55 UTC
- **Edited time:** January 08, 2024, 20:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2FastLaunchFullAccess

Description: This policy grants full access to EC2 Fast Launch actions

EC2FastLaunchFullAccess is an [AWS managed policy](#).

Using this policy

You can attach EC2FastLaunchFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 13, 2024, 22:45 UTC
- **Edited time:** May 13, 2024, 22:45 UTC
- **ARN:** arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2FastLaunchServiceRolePolicy

Description: Policy grants ec2fastlaunch to prepare and manage preprovisioned snapshots in customer's account & publish related metrics.

EC2FastLaunchServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 10, 2022, 13:08 UTC
- **Edited time:** January 10, 2022, 13:08 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2FleetTimeShiftableServiceRolePolicy

Description: Policy granting permissions to EC2 Fleet to launch instances in the future.

EC2FleetTimeShiftableServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 23, 2019, 19:47 UTC
- **Edited time:** December 23, 2019, 19:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
      }
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Description: Permissions need by EC2 Image Builder to perform a cross account distribution.

Ec2ImageBuilderCrossAccountDistributionAccess is an [AWS managed policy](#).

Using this policy

You can attach Ec2ImageBuilderCrossAccountDistributionAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 30, 2020, 19:22 UTC
- **Edited time:** September 30, 2020, 19:22 UTC
- **ARN:** arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2ImageBuilderLifecycleExecutionPolicy

Description: The EC2ImageBuilderLifecycleExecutionPolicy policy grants permissions for Image Builder to perform actions such as deprecate or delete Image Builder image resources and their underlying resources (AMIs, snapshots) to support automated rules for image lifecycle management tasks.

EC2ImageBuilderLifecycleExecutionPolicy is an [AWS managed policy](#).

Using this policy

You can attach EC2ImageBuilderLifecycleExecutionPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 16, 2023, 23:23 UTC
- **Edited time:** November 16, 2023, 23:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "EC2DeleteSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "EC2TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*::snapshot/*",
      "arn:aws:ec2:*::image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "DeprecatedBy"
      }
    }
  },
  {
    "Sid" : "ECRImagePermission",
    "Effect" : "Allow",
    "Action" : [
      "ecr:BatchGetImage",
      "ecr:BatchDeleteImage"
    ]
  }
}
```

```
    ],
    "Resource" : "arn:aws:ecr:*:*:repository/*",
    "Condition" : {
      "StringEquals" : {
        "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "ImageBuilderEC2TagServicePermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "tag:GetResources",
      "imagebuilder:DeleteImage"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2InstanceConnect

Description: Allows customers to call EC2 Instance Connect to publish ephemeral keys to their EC2 instances and connect via ssh or the EC2 Instance Connect CLI.

EC2InstanceConnect is an [AWS managed policy](#).

Using this policy

You can attach EC2InstanceConnect to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 27, 2019, 18:53 UTC
- **Edited time:** June 27, 2019, 18:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/EC2InstanceConnect`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Ec2InstanceConnectEndpoint

Description: EC2 Instance Connect endpoint policy to manage EC2 Instance Connect endpoints created by the customer

Ec2InstanceConnectEndpoint is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 24, 2023, 20:19 UTC
- **Edited time:** January 24, 2023, 20:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
      ]
    }
  }
}
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2InstanceProfileForImageBuilder

Description: EC2 Instance profile for Image Builder service.

EC2InstanceProfileForImageBuilder is an [AWS managed policy](#).

Using this policy

You can attach `EC2InstanceProfileForImageBuilder` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 01, 2019, 19:08 UTC
- **Edited time:** August 27, 2020, 16:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

Description: EC2 Instance profile for building container images with EC2 Image Builder. This policy grants the user broad permissions to upload ECR images.

EC2InstanceProfileForImageBuilderECRContainerBuilds is an [AWS managed policy](#).

Using this policy

You can attach `EC2InstanceProfileForImageBuilderECRContainerBuilds` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 11, 2020, 19:48 UTC
- **Edited time:** December 11, 2020, 19:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ECRReplicationServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by ECR Replication

ECRReplicationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 04, 2020, 22:11 UTC
- **Edited time:** December 04, 2020, 22:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"    
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ECRTemplateServiceRolePolicy

Description: Allows actions to be performed when using AWS ECR repository creation templates

ECRTemplateServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 19, 2024, 23:11 UTC
- **Edited time:** June 19, 2024, 23:11 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElastiCacheServiceRolePolicy

Description: This policy allows ElastiCache to manage AWS resources on your behalf as necessary for managing your cache

ElastiCacheServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 07, 2017, 17:50 UTC
- **Edited time:** November 28, 2023, 03:05 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"
}

```

```
}  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElasticLoadBalancingFullAccess

Description: Provides full access to Amazon ElasticLoadBalancing, and limited access to other services necessary to provide ElasticLoadBalancing features.

ElasticLoadBalancingFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ElasticLoadBalancingFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 20, 2018, 20:42 UTC
- **Edited time:** November 29, 2022, 01:45 UTC
- **ARN:** arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElasticLoadBalancingReadOnly

Description: Provides read only access to Amazon ElasticLoadBalancing and dependent services

ElasticLoadBalancingReadOnly is an [AWS managed policy](#).

Using this policy

You can attach ElasticLoadBalancingReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 20, 2018, 20:17 UTC
- **Edited time:** November 26, 2023, 18:15 UTC
- **ARN:** arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalActivationsDownloadSoftwareAccess

Description: Access to view purchased assets and download related software and kickstart files

ElementalActivationsDownloadSoftwareAccess is an [AWS managed policy](#).

Using this policy

You can attach ElementalActivationsDownloadSoftwareAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** September 08, 2020, 17:26 UTC
- **Edited time:** September 08, 2020, 17:26 UTC
- **ARN:** arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalActivationsFullAccess

Description: Full access to view and take action on Elemental Appliances and Software purchased assets

ElementalActivationsFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ElementalActivationsFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 04, 2020, 21:00 UTC

- **Edited time:** June 04, 2020, 21:00 UTC
- **ARN:** `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalActivationsGenerateLicenses

Description: Access to view purchased assets and generate software licenses for pending activations

ElementalActivationsGenerateLicenses is an [AWS managed policy](#).

Using this policy

You can attach ElementalActivationsGenerateLicenses to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 28, 2020, 18:28 UTC
- **Edited time:** August 28, 2020, 18:28 UTC
- **ARN:** arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalActivationsReadOnlyAccess

Description: Read-only access to the detailed list of purchased assets associated to the AWS account of the user

ElementalActivationsReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach ElementalActivationsReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 28, 2020, 16:51 UTC
- **Edited time:** August 28, 2020, 16:51 UTC
- **ARN:** arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "elemental-activations:Get*"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalAppliancesSoftwareFullAccess

Description: Full access to view and take action on Elemental Appliances and Software quotes and orders

ElementalAppliancesSoftwareFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ElementalAppliancesSoftwareFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 31, 2019, 16:28 UTC
- **Edited time:** February 05, 2021, 21:01 UTC
- **ARN:** arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalAppliancesSoftwareReadOnlyAccess

Description: Read-only access to view Elemental Appliances and Software quotes and orders

ElementalAppliancesSoftwareReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `ElementalAppliancesSoftwareReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 01, 2020, 22:31 UTC
- **Edited time:** April 01, 2020, 22:31 UTC
- **ARN:** `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ElementalSupportCenterFullAccess

Description: Full access to view and take action on Elemental Appliance and Software support cases and product support content

ElementalSupportCenterFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ElementalSupportCenterFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 25, 2020, 18:08 UTC
- **Edited time:** February 05, 2021, 21:02 UTC
- **ARN:** arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "elemental-support-cases:*",
      "elemental-support-content:*",
      "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

EMRDescribeClusterPolicyForEMRWAL

Description: This policy grants read-only permissions that allow the WAL service for Amazon EMR to find and return the status of a cluster

EMRDescribeClusterPolicyForEMRWAL is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 15, 2023, 23:30 UTC
- **Edited time:** June 15, 2023, 23:30 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

FMSServiceRolePolicy

Description: Access policy to allow FM service linked role to perform FM-related actions on FM-managed resources within a customer AWS Organization account.

FMSServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** March 28, 2018, 23:01 UTC
- **Edited time:** April 22, 2024, 19:12 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

Policy version

Policy version: v29 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

FSxDeleteServiceLinkedRoleAccess

Description: Allows Amazon FSx to delete its Service Linked Roles for Amazon S3 access

FSxDeleteServiceLinkedRoleAccess is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 28, 2018, 10:40 UTC
- **Edited time:** November 28, 2018, 10:40 UTC

- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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_*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GameLiftGameServerGroupPolicy

Description: Policy to allow Gamelift GameServerGroups to manage customer resources

GameLiftGameServerGroupPolicy is an [AWS managed policy](#).

Using this policy

You can attach `GameLiftGameServerGroupPolicy` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 03, 2020, 23:12 UTC
- **Edited time:** May 13, 2020, 17:27 UTC
- **ARN:** `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
```

```
    "autoscaling:SetInstanceProtection",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SuspendProcesses",
    "autoscaling:DetachInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/GameLift" : "GameServerGroups"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "sns:Publish",
  "Resource" : [
    "arn*:sns:*:*:ActivatingLifecycleHookTopic-*",
    "arn*:sns:*:*:TerminatingLifecycleHookTopic-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/GameLift"
    }
  }
}
]
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GlobalAcceleratorFullAccess

Description: Allow GlobalAccelerator Users full Access to all APIs

GlobalAcceleratorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach GlobalAcceleratorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 02:44 UTC
- **Edited time:** December 04, 2020, 19:17 UTC
- **ARN:** arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```

"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"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GlobalAcceleratorReadOnlyAccess

Description: Allow GlobalAccelerator Users Access to Read Only APIs

GlobalAcceleratorReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach GlobalAcceleratorReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 02:41 UTC
- **Edited time:** November 27, 2018, 02:41 UTC
- **ARN:** `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",

```



```
    "globalaccelerator:List*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GreengrassOTAUpdateArtifactAccess

Description: Provides read access to the Greengrass OTA Update artifacts in all Greengrass regions

GreengrassOTAUpdateArtifactAccess is an [AWS managed policy](#).

Using this policy

You can attach GreengrassOTAUpdateArtifactAccess to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 29, 2017, 18:11 UTC
- **Edited time:** December 18, 2018, 00:59 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GroundTruthSyntheticConsoleFullAccess

Description: This policy grants permissions needed to use all features of the SageMaker Ground Truth Synthetic Console.

GroundTruthSyntheticConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach GroundTruthSyntheticConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 25, 2022, 15:58 UTC
- **Edited time:** August 25, 2022, 15:58 UTC
- **ARN:** arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

GroundTruthSyntheticConsoleReadOnlyAccess

Description: This policy grants read-only access to SageMaker Ground Truth Synthetic via the AWS Management Console.

GroundTruthSyntheticConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach GroundTruthSyntheticConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** August 25, 2022, 15:58 UTC
- **Edited time:** August 25, 2022, 15:58 UTC
- **ARN:** `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Health_OrganizationsServiceRolePolicy

Description: AWS Health policy to enable Organizational View feature

Health_OrganizationsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 16, 2019, 13:28 UTC
- **Edited time:** February 06, 2024, 16:07 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMAccessAdvisorReadOnly

Description: This policy grants access to read all access information provided by IAM access advisor such as service last accessed information.

IAMAccessAdvisorReadOnly is an [AWS managed policy](#).

Using this policy

You can attach IAMAccessAdvisorReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 21, 2019, 19:33 UTC

- **Edited time:** June 21, 2019, 19:33 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMAccessAnalyzerFullAccess

Description: Provides full access to IAM Access Analyzer

IAMAccessAnalyzerFullAccess is an [AWS managed policy](#).

Using this policy

You can attach IAMAccessAnalyzerFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 02, 2019, 17:12 UTC
- **Edited time:** December 02, 2019, 17:12 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMAccessAnalyzerReadOnlyAccess

Description: Provides read only access to IAM Access Analyzer resources

IAMAccessAnalyzerReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach IAMAccessAnalyzerReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 02, 2019, 17:12 UTC
- **Edited time:** November 27, 2023, 02:24 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{  
  "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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMFullAccess

Description: Provides full access to IAM via the AWS Management Console.

IAMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach IAMFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** June 21, 2019, 19:40 UTC

- **ARN:** `arn:aws:iam::aws:policy/IAMFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)

- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMReadOnlyAccess

Description: Provides read only access to IAM via the AWS Management Console.

IAMReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach IAMReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:40 UTC
- **Edited time:** January 25, 2018, 19:11 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMReadOnlyAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*"
      ]
    }
  ]
}
```

```
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMSelfManageServiceSpecificCredentials

Description: Allows an IAM user to manage their own Service Specific Credentials.

IAMSelfManageServiceSpecificCredentials is an [AWS managed policy](#).

Using this policy

You can attach IAMSelfManageServiceSpecificCredentials to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 22, 2016, 17:25 UTC
- **Edited time:** December 22, 2016, 17:25 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMUserChangePassword

Description: Provides the ability for an IAM user to change their own password.

IAMUserChangePassword is an [AWS managed policy](#).

Using this policy

You can attach IAMUserChangePassword to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 15, 2016, 00:25 UTC
- **Edited time:** November 15, 2016, 23:18 UTC
- **ARN:** `arn:aws:iam::aws:policy/IAMUserChangePassword`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IAMUserSSHKeys

Description: Provides the ability for an IAM user to manage their own SSH keys.

IAMUserSSHKeys is an [AWS managed policy](#).

Using this policy

You can attach IAMUserSSHKeys to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** July 09, 2015, 17:08 UTC
- **Edited time:** July 09, 2015, 17:08 UTC
- **ARN:** arn:aws:iam::aws:policy/IAMUserSSHKeys

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{  
  "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}"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IVSFullAccess

Description: Provides full access to Interactive Video Service (IVS), Also included permissions for dependent services, needed for full access to the ivs console.

IVSFullAccess is an [AWS managed policy](#).

Using this policy

You can attach IVSFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 13, 2023, 21:20 UTC
- **Edited time:** December 13, 2023, 21:20 UTC

- **ARN:** `arn:aws:iam::aws:policy/IVSFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IVSReadOnlyAccess

Description: Provides read-only access to IVS Low-Latency and Real-Time streaming APIs

IVSReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `IVSReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** December 05, 2023, 18:00 UTC
- **Edited time:** February 16, 2024, 18:03 UTC
- **ARN:** `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

IVSRecordToS3

Description: Service Linked Role to perform S3 PutObject to recording IVS live streams

IVSRecordToS3 is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** December 05, 2020, 00:10 UTC
- **Edited time:** December 05, 2020, 00:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

KafkaConnectServiceRolePolicy

Description: This policy grants Kafka Connect permission to manage AWS resources on your behalf.

KafkaConnectServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 07, 2021, 13:12 UTC
- **Edited time:** September 07, 2021, 13:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}

```



```
}  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

KafkaServiceRolePolicy

Description: IAM service linked role policy for Kafka.

KafkaServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 15, 2018, 23:31 UTC
- **Edited time:** April 28, 2023, 00:39 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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_*"
    }
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

KeyspacesReplicationServiceRolePolicy

Description: Permissions required by Keyspaces for cross-region data replication

KeyspacesReplicationServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 02, 2023, 16:15 UTC
- **Edited time:** May 02, 2023, 16:15 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

LakeFormationDataAccessServiceRolePolicy

Description: Policy to grant temporary data access to Lake Formation resources

LakeFormationDataAccessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 20, 2019, 20:46 UTC
- **Edited time:** February 06, 2024, 18:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3::*:*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

LexBotPolicy

Description: Policy for AWS Lex Bot use case

LexBotPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** February 17, 2017, 22:18 UTC
- **Edited time:** November 13, 2019, 22:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "polly:SynthesizeSpeech"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "comprehend:DetectSentiment"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

LexChannelPolicy

Description: Policy for AWS Lex Channel use case

LexChannelPolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy

- **Creation time:** February 17, 2017, 23:23 UTC
- **Edited time:** February 17, 2017, 23:23 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

LightsailExportAccess

Description: AWS Lightsail service linked role policy which grants permissions to export resources

LightsailExportAccess is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 28, 2018, 16:35 UTC
- **Edited time:** January 15, 2022, 01:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MediaConnectGatewayInstanceRolePolicy

Description: This policy grants permission to register MediaConnect Gateway Instances to a MediaConnect Gateway.

MediaConnectGatewayInstanceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach MediaConnectGatewayInstanceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 22, 2023, 20:43 UTC
- **Edited time:** March 22, 2023, 20:43 UTC
- **ARN:** arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediacconnect:DiscoverGatewayPollEndpoint",
        "mediacconnect:PollGateway",
        "mediacconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MediaPackageServiceRolePolicy

Description: Allows MediaPackage to publish logs to CloudWatch

MediaPackageServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** September 18, 2020, 17:45 UTC
- **Edited time:** September 18, 2020, 17:45 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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/*"  
  }  
]  
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MemoryDBServiceRolePolicy

Description: This policy allows MemoryDB to manage AWS resources on your behalf as necessary for managing your resources.

MemoryDBServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 17, 2021, 22:34 UTC
- **Edited time:** August 18, 2021, 23:48 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MigrationHubDMSAccessServiceRolePolicy

Description: Policy for Database Migration Service to assume role in customer's account to call Migration Hub

MigrationHubDMSAccessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 12, 2019, 17:50 UTC
- **Edited time:** October 07, 2019, 17:57 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MigrationHubServiceRolePolicy

Description: Allows Migration Hub to call Application Discovery Service on your behalf

MigrationHubServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 12, 2019, 17:22 UTC
- **Edited time:** August 06, 2020, 18:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
      "*"
    ]
  }
]
}

```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MigrationHubSMSAccessServiceRolePolicy

Description: Policy for Server Migration Service to assume role in customer's account to call Migration Hub

MigrationHubSMSAccessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 12, 2019, 18:30 UTC
- **Edited time:** October 07, 2019, 18:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

MonitronServiceRolePolicy

Description: Policy for AWS Monitron service linked role granting access to required customer resources.

MonitronServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 02, 2022, 19:22 UTC
- **Edited time:** May 02, 2022, 19:22 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

NeptuneConsoleFullAccess

Description: Provides full access to manage Amazon Neptune using the AWS Management Console. Note this policy also grants full access to publish on all SNS topics within the account, permissions to create and edit Amazon EC2 instances and VPC configurations, permissions to view and list keys on Amazon KMS, and full access to Amazon RDS. For more information, see <https://aws.amazon.com/neptune/faqs/>.

NeptuneConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach NeptuneConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 19, 2018, 21:35 UTC
- **Edited time:** November 30, 2023, 07:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

NeptuneFullAccess

Description: Provides full access to Amazon Neptune. Note this policy also grants full access to publish on all SNS topics within the account and full access to Amazon RDS. For more information, see <https://aws.amazon.com/neptune/faqs/>.

NeptuneFullAccess is an [AWS managed policy](#).

Using this policy

You can attach NeptuneFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 30, 2018, 19:17 UTC
- **Edited time:** January 22, 2024, 16:32 UTC

- **ARN:** `arn:aws:iam::aws:policy/NeptuneFullAccess`

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
    "*"
  ]
}

```

```
    }  
  ]  
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

NeptuneGraphReadOnlyAccess

Description: Provides read only access to all Amazon Neptune Analytics resources along with read only permissions for dependent services.

NeptuneGraphReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach NeptuneGraphReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 30, 2023, 07:32 UTC
- **Edited time:** November 30, 2023, 07:32 UTC
- **ARN:** `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:*"
  ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

NeptuneReadOnlyAccess

Description: Provides read only access to Amazon Neptune. Note that this policy also grants access to Amazon RDS resources. For more information, see <https://aws.amazon.com/neptune/faqs/>.

NeptuneReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach NeptuneReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 30, 2018, 19:16 UTC

- **Edited time:** January 22, 2024, 16:33 UTC
- **ARN:** arn:aws:iam::aws:policy/NeptuneReadOnlyAccess

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : [
        "*"
    ]
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

NetworkAdministrator

Description: Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

NetworkAdministrator is an [AWS managed policy](#).

Using this policy

You can attach NetworkAdministrator to your users, groups, and roles.

Policy details

- **Type:** Job function policy

- **Creation time:** November 10, 2016, 17:31 UTC
- **Edited time:** June 26, 2024, 16:53 UTC
- **ARN:** arn:aws:iam::aws:policy/job-function/NetworkAdministrator

Policy version

Policy version: v12 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
```



```
"ec2:CreateCustomerGateway",
"ec2:CreateDefaultSubnet",
"ec2:CreateDefaultVpc",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateFlowLogs",
"ec2:CreateInternetGateway",
"ec2:CreateNatGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkAclEntry",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreatePlacementGroup",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpcEndpointConnectionNotification",
"ec2:CreateVpcEndpointServiceConfiguration",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteCarrierGateway",
"ec2>DeleteEgressOnlyInternetGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2>DeletePlacementGroup",
"ec2>DeleteSubnet",
"ec2>DeleteTags",
"ec2>DeleteVpc",
"ec2>DeleteVpcEndpointConnectionNotifications",
"ec2>DeleteVpcEndpointServiceConfigurations",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteVpnConnection",
"ec2>DeleteVpnConnectionRoute",
"ec2>DeleteVpnGateway",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
```

```
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeIpv6Pools",
"ec2:DescribeKeyPairs",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
```

```
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:DisassociateSubnetCidrBlock",
"ec2:DisassociateVpcCidrBlock",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVpcClassicLinkDnsSupport",
"ec2:GetVpnConnectionDeviceSampleConfiguration",
"ec2:GetVpnConnectionDeviceTypes",
"ec2:GetVpnTunnelReplacementStatus",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVpcAttribute",
"ec2:ModifyVpcEndpoint",
"ec2:ModifyVpcEndpointConnectionNotification",
"ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:ModifyVpcEndpointServicePermissions",
"ec2:ModifyVpcPeeringConnectionOptions",
"ec2:ModifyVpcTenancy",
"ec2:ModifyVpnConnection",
"ec2:ModifyVpnConnectionOptions",
"ec2:ModifyVpnTunnelCertificate",
"ec2:ModifyVpnTunnelOptions",
"ec2:MoveAddressToVpc",
"ec2:RejectVpcEndpointConnections",
"ec2:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceNetworkAclEntry",
"ec2:ReplaceRoute",
"ec2:ReplaceRouteTableAssociation",
"ec2:ReplaceVpnTunnel",
"ec2:ResetNetworkInterfaceAttribute",
"ec2:RestoreAddressToClassic",
"ec2:UnassignIpv6Addresses",
"ec2:UnassignPrivateIpAddresses",
"ec2:UpdateSecurityGroupRuleDescriptionsEgress",
"ec2:UpdateSecurityGroupRuleDescriptionsIngress",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticloadbalancing:*",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
```

```
    "logs:GetLogEvents",
    "route53:*",
    "route53domains:*",
    "sns:CreateTopic",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowVPCPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AcceptVpcPeeringConnection",
    "ec2: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" : [
    "*"
  ]
},
{
  "Sid" : "AllowLocalGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:CreateLocalGatewayRoute",
    "ec2:CreateLocalGatewayRouteTableVpcAssociation",
    "ec2>DeleteLocalGatewayRoute",
    "ec2>DeleteLocalGatewayRouteTableVpcAssociation",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeLocalGateways",
    "ec2:SearchLocalGatewayRoutes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DiscoverBuckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "s3:ListBucket"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DiscoverFlowLogRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/flow-logs-*"
},
{
  "Sid" : "NetworkmanagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "networkmanager:*"
  ],
  "Resource" : "*"
},

```

```

{
  "Sid" : "TransitGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AcceptTransitGatewayVpcAttachment",
    "ec2:AssociateTransitGatewayRouteTable",
    "ec2:CreateTransitGateway",
    "ec2:CreateTransitGatewayRoute",
    "ec2:CreateTransitGatewayRouteTable",
    "ec2:CreateTransitGatewayVpcAttachment",
    "ec2>DeleteTransitGateway",
    "ec2>DeleteTransitGatewayRoute",
    "ec2>DeleteTransitGatewayRouteTable",
    "ec2>DeleteTransitGatewayVpcAttachment",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2: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" : "*"
},
{
  "Sid" : "AllowTransitGatewaySLRCreation",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "transitgateway.amazonaws.com"
      ]
    }
  }
}

```

```
    ]
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

OAMFullAccess

Description: Provides full access to CloudWatch Observability Access Manager

OAMFullAccess is an [AWS managed policy](#).

Using this policy

You can attach OAMFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 13:38 UTC
- **Edited time:** November 27, 2022, 13:38 UTC
- **ARN:** `arn:aws:iam::aws:policy/OAMFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

OAMReadOnlyAccess

Description: Provides Read Only access to CloudWatch Observability Access Manager

OAMReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach OAMReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2022, 13:29 UTC
- **Edited time:** November 27, 2022, 13:29 UTC

- **ARN:** `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

OpensearchIngestionSelfManagedVpcePolicy

Description: Allows Amazon OpenSearch Ingestion to describe network resources and write service metrics to cloudwatch

OpensearchIngestionSelfManagedVpcePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 10, 2024, 19:59 UTC
- **Edited time:** June 10, 2024, 19:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

PartnerCentralAccountManagementUserRoleAssociation

Description: Provides access to associate and dissociate partner central users with IAM roles

PartnerCentralAccountManagementUserRoleAssociation is an [AWS managed policy](#).

Using this policy

You can attach PartnerCentralAccountManagementUserRoleAssociation to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 10, 2023, 02:03 UTC
- **Edited time:** November 10, 2023, 02:03 UTC
- **ARN:** arn:aws:iam::aws:policy/
PartnerCentralAccountManagementUserRoleAssociation

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

PowerUserAccess

Description: Provides full access to AWS services and resources, but does not allow management of Users and groups.

PowerUserAccess is an [AWS managed policy](#).

Using this policy

You can attach PowerUserAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** July 06, 2023, 22:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/PowerUserAccess`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

QBusinessServiceRolePolicy

Description: Grants permissions to AWS services and Resources used or managed by Amazon Q. QBusinessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 29, 2024, 16:05 UTC
- **Edited time:** April 29, 2024, 16:05 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}"
    }
  }
}
]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Description: Policy used by QuickSight team to access customer data produced by S3 Storage Management Analytics.

QuickSightAccessForS3StorageManagementAnalyticsReadOnly is an [AWS managed policy](#).

Using this policy

You can attach QuickSightAccessForS3StorageManagementAnalyticsReadOnly to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 12, 2017, 18:18 UTC
- **Edited time:** October 08, 2019, 23:53 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

RDSCloudHsmAuthorizationRole

Description: Default policy for the Amazon RDS service role.

RDSCloudHsmAuthorizationRole is an [AWS managed policy](#).

Using this policy

You can attach RDSCloudHsmAuthorizationRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** September 26, 2019, 22:14 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ReadOnlyAccess

Description: Provides read-only access to AWS services and resources.

ReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `ReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** June 21, 2024, 20:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/ReadOnlyAccess`

Policy version

Policy version: v114 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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:DescribeBotReplica",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:Get*",
"lex:ListBotAliasReplicas",
"lex:ListBotAliases",
```



```
"lex:ListBotChannels",
"lex:ListBotLocales",
"lex:ListBotReplicas",
"lex:ListBotVersionReplicas",
"lex: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:ListPaymentInstruments",
"payments:ListPaymentPreferences",
"payments:ListTagsForResource",
"pca-connector-ad:GetConnector",
"pca-connector-ad:GetDirectoryRegistration",
"pca-connector-ad:GetServicePrincipalName",
"pca-connector-ad:GetTemplate",
"pca-connector-ad:GetTemplateGroupAccessControlEntry",
"pca-connector-ad:ListConnectors",
"pca-connector-ad:ListDirectoryRegistrations",
"pca-connector-ad:ListServicePrincipalNames",
"pca-connector-ad:ListTagsForResource",
"pca-connector-ad:ListTemplateGroupAccessControlEntries",
"pca-connector-ad:ListTemplates",
"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*",
```

```
"resiliencyhub:DescribeApp",
"resiliencyhub:DescribeAppAssessment",
"resiliencyhub:DescribeAppVersion",
"resiliencyhub:DescribeAppVersionAppComponent",
"resiliencyhub:DescribeAppVersionResource",
"resiliencyhub:DescribeAppVersionResourcesResolutionStatus",
"resiliencyhub:DescribeAppVersionTemplate",
"resiliencyhub:DescribeDraftAppVersionResourcesImportStatus",
"resiliencyhub:DescribeResiliencyPolicy",
"resiliencyhub:ListAlarmRecommendations",
"resiliencyhub:ListAppAssessmentComplianceDrifts",
"resiliencyhub:ListAppAssessments",
"resiliencyhub:ListAppComponentCompliances",
"resiliencyhub:ListAppComponentRecommendations",
"resiliencyhub:ListAppInputSources",
"resiliencyhub:ListApps",
"resiliencyhub:ListAppVersionAppComponents",
"resiliencyhub:ListAppVersionResourceMappings",
"resiliencyhub:ListAppVersionResources",
"resiliencyhub:ListAppVersions",
"resiliencyhub:ListRecommendationTemplates",
"resiliencyhub:ListResiliencyPolicies",
"resiliencyhub:ListSopRecommendations",
"resiliencyhub:ListSuggestedResiliencyPolicies",
"resiliencyhub:ListTagsForResource",
"resiliencyhub:ListTestRecommendations",
"resiliencyhub:ListUnsupportedAppVersionResources",
"resource-explorer-2:BatchGetView",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:GetView",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"resource-explorer-2:Search",
"resource-groups:Get*",
"resource-groups:List*",
"resource-groups:Search*",
"robomaker:BatchDescribe*",
"robomaker:Describe*",
"robomaker:Get*",
"robomaker:List*",
"route53-recovery-cluster:Get*",
```

```
"route53-recovery-cluster:ListRoutingControls",
"route53-recovery-control-config:Describe*",
"route53-recovery-control-config:GetResourcePolicy",
"route53-recovery-control-config:List*",
"route53-recovery-readiness:Get*",
"route53-recovery-readiness:List*",
"route53:Get*",
"route53:List*",
"route53:Test*",
"route53domains:Check*",
"route53domains:Get*",
"route53domains:List*",
"route53domains:View*",
"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" : "*"
}
]
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ResourceGroupsandTagEditorFullAccess

Description: Provides full access to Resource Groups and Tag Editor.

ResourceGroupsandTagEditorFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ResourceGroupsandTagEditorFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** August 10, 2023, 13:29 UTC
- **ARN:** arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"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" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ResourceGroupsandTagEditorReadOnlyAccess

Description: Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.

ResourceGroupsandTagEditorReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach ResourceGroupsandTagEditorReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:39 UTC
- **Edited time:** August 10, 2023, 13:42 UTC
- **ARN:** `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```


Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ResourceGroupsServiceRolePolicy

Description: Allows AWS Resource Groups to query the AWS services that own your resources to keep the group up-to-date

ResourceGroupsServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** January 05, 2023, 16:57 UTC
- **Edited time:** January 05, 2023, 16:57 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

Description: Allows the OpenShift Amazon EBS Container Storage Interface (CSI) Driver Operator to install and maintain the Amazon EBS CSI driver on a Red Hat OpenShift Service on AWS (ROSA) cluster. The Amazon EBS CSI driver allows ROSA clusters to manage the lifecycle of Amazon EBS volumes for persistent volumes.

ROSAAmazonEBSCSIDriverOperatorPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAAmazonEBSCSIDriverOperatorPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2023, 22:36 UTC

- **Edited time:** April 20, 2023, 22:36 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    ]
}
}
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSACloudNetworkConfigOperatorPolicy

Description: Allows the OpenShift Cloud Network Config Controller Operator to provision and manage networking resources for use by the Red Hat OpenShift Service on AWS (ROSA) cluster networking overlay. The OpenShift Cloud Network Operator interfaces with AWS APIs on behalf of the network plugins via CustomResourceDefinitions. The operator uses these policy permissions to manage private IP addresses for Amazon EC2 instances as part of the ROSA cluster.

ROSACloudNetworkConfigOperatorPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSACloudNetworkConfigOperatorPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2023, 22:34 UTC
- **Edited time:** April 20, 2023, 22:34 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
        }
      }
    }
  ]
}
```

```
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAControlPlaneOperatorPolicy

Description: Allows Red Hat OpenShift Service on AWS (ROSA) control plane to manage ROSA cluster Amazon EC2 and Amazon Route 53 resources.

ROSAControlPlaneOperatorPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAControlPlaneOperatorPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 24, 2023, 23:02 UTC
- **Edited time:** June 30, 2023, 21:12 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    ]
  }
}
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAImageRegistryOperatorPolicy

Description: Allows the OpenShift Image Registry Operator to provision and manage Amazon S3 buckets and objects for use by the Red Hat OpenShift Service on AWS (ROSA) in-cluster image registry to satisfy ROSA storage requirements. The OpenShift Image Registry Operator installs and maintains the internal registry of a Red Hat OpenShift cluster.

ROSAImageRegistryOperatorPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAImageRegistryOperatorPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** April 27, 2023, 20:13 UTC
- **Edited time:** December 12, 2023, 19:53 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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}/*"
    ]
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAIngressOperatorPolicy

Description: Allows the OpenShift Ingress Operator to provision and manage load balancers and domain name system (DNS) configurations for Red Hat OpenShift Service on AWS (ROSA) clusters. The policy allows read access to tag values, which the operator filters for Route 53 resources to discover hosted zones.

ROSAIngressOperatorPolicy is an [AWS managed policy](#).

Using this policy

You can attach `R0SAIngressOperatorPolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2023, 22:37 UTC
- **Edited time:** April 20, 2023, 22:37 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/R0SAIngressOperatorPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      ]
    }
  }
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAInstallerPolicy

Description: Allows the Red Hat OpenShift Service on AWS (ROSA) installer to manage AWS resources that support ROSA cluster installation. This includes managing instance profiles for ROSA worker nodes.

ROSAInstallerPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAInstallerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 06, 2023, 21:00 UTC
- **Edited time:** April 24, 2024, 19:49 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAKMSPProviderPolicy

Description: Allows the built-in ROSA AWS Encryption Provider to manage AWS Key Management Service (KMS) keys to support etcd data encryption using a customer provided AWS KMS key. The policy allows encryption and decryption of data using KMS keys.

ROSAKMSPProviderPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAKMSPProviderPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 27, 2023, 20:10 UTC
- **Edited time:** April 27, 2023, 20:10 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSAKMSPProviderPolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "VolumeEncryption",
    "Effect" : "Allow",
    "Action" : [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat" : "true"
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAKubeControllerPolicy

Description: Allows the ROSA Kubernetes controller to manage Amazon EC2, Elastic Load Balancing (ELB), and AWS Key Management Service (KMS) resources for a ROSA cluster.

ROSAKubeControllerPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSAKubeControllerPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 27, 2023, 20:09 UTC
- **Edited time:** October 16, 2023, 18:17 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAManageSubscription

Description: This policy provides the permissions required to manage the Red Hat OpenShift Service on AWS (ROSA) subscription.

ROSAManageSubscription is an [AWS managed policy](#).

Using this policy

You can attach ROSAManageSubscription to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 11, 2022, 20:58 UTC
- **Edited time:** August 04, 2023, 19:59 UTC
- **ARN:** `arn:aws:iam::aws:policy/ROSAManageSubscription`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSANodePoolManagementPolicy

Description: Allows Red Hat OpenShift Service on AWS (ROSA) to manage cluster EC2 instances as worker nodes, including permission to configure security groups and tag instances and volumes. This policy also allows for the use of EC2 instances with disk encryption provided by AWS Key Management Service (KMS) keys.

ROSANodePoolManagementPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSANodePoolManagementPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy

- **Creation time:** June 08, 2023, 20:48 UTC
- **Edited time:** May 02, 2024, 14:01 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSASRESupportPolicy

Description: Provides ROSA site reliability engineering (SRE) the permissions needed to initially observe, diagnose, and support AWS resources associated with Red Hat OpenShift Service on AWS (ROSA) clusters, including the ability to change ROSA cluster node state.

ROSASRESupportPolicy is an [AWS managed policy](#).

Using this policy

You can attach ROSASRESupportPolicy to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** June 01, 2023, 14:36 UTC
- **Edited time:** April 10, 2024, 20:51 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ROSAWorkerInstancePolicy

Description: Allows Red Hat OpenShift Service on AWS (ROSA) worker nodes in your account read-only access to Amazon EC2 instances and AWS Regions for compute node lifecycle management.

ROSAWorkerInstancePolicy is an [AWS managed policy](#).

Using this policy

You can attach `ROSASWorkerInstancePolicy` to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** April 20, 2023, 22:35 UTC
- **Edited time:** April 20, 2023, 22:35 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/ROSASWorkerInstancePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Route53RecoveryReadinessServiceRolePolicy

Description: Service Linked Role Policy for Route 53 Recovery Readiness

Route53RecoveryReadinessServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** July 15, 2021, 16:06 UTC
- **Edited time:** February 14, 2023, 18:08 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

Route53ResolverServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Route53 Resolver

Route53ResolverServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 12, 2020, 17:47 UTC
- **Edited time:** August 12, 2020, 17:47 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

S3StorageLensServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by S3 Storage Lens

S3StorageLensServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 18, 2020, 18:15 UTC
- **Edited time:** November 18, 2020, 18:15 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SecretsManagerReadWrite

Description: Provides read/write access to AWS Secrets Manager via the AWS Management Console. Note: this excludes IAM actions, so combine with IAMFullAccess if rotation configuration is required.

SecretsManagerReadWrite is an [AWS managed policy](#).

Using this policy

You can attach SecretsManagerReadWrite to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** April 04, 2018, 18:05 UTC
- **Edited time:** February 22, 2024, 18:12 UTC
- **ARN:** arn:aws:iam::aws:policy/SecretsManagerReadWrite

Policy version

Policy version: v5 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{  
  "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-*/*"
    ]
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SecurityAudit

Description: The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SecurityAudit is an [AWS managed policy](#).

Using this policy

You can attach SecurityAudit to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** April 05, 2024, 17:32 UTC
- **ARN:** arn:aws:iam::aws:policy/SecurityAudit

Policy version

Policy version: v42 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
  ]
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SecurityLakeServiceLinkedRole

Description: This policy grants permissions to operate the Amazon Security Lake service on your behalf

SecurityLakeServiceLinkedRole is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 29, 2022, 14:03 UTC
- **Edited time:** April 19, 2024, 16:00 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
            ]
        }
    }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServerMigration_ServiceRole

Description: Permissions to allow the AWS Server Migration Service to migrate VMs to EC2: allows the Server Migration Service to place the migrated resources into the customer's EC2 account.

ServerMigration_ServiceRole is an [AWS managed policy](#).

Using this policy

You can attach ServerMigration_ServiceRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** August 11, 2020, 20:41 UTC
- **Edited time:** October 15, 2020, 17:26 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*/*"
      }
    }
  }
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServerMigrationConnector

Description: Permissions to allow the AWS Server Migration Connector to migrate VMs to EC2. Allows communication with the AWS Server Migration Service, read/write access to S3 buckets starting with 'sms-b-' and 'import-to-ec2-' as well as the buckets used for AWS Server Migration Connector upgrade, AWS Server Migration Connector registration with AWS, and metrics upload to AWS.

ServerMigrationConnector is an [AWS managed policy](#).

Using this policy

You can attach ServerMigrationConnector to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** October 24, 2016, 21:45 UTC
- **Edited time:** October 24, 2016, 21:45 UTC
- **ARN:** arn:aws:iam::aws:policy/ServerMigrationConnector

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServerMigrationServiceConsoleFullAccess

Description: Required permissions to use all features of the Server Migration Service Console

ServerMigrationServiceConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ServerMigrationServiceConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** May 09, 2020, 17:18 UTC
- **Edited time:** July 20, 2020, 22:00 UTC
- **ARN:** arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServerMigrationServiceLaunchRole

Description: Permissions to allow the AWS Server Migration Service to create and update relevant AWS resources into the customer's AWS account for launching migrated servers and applications.

ServerMigrationServiceLaunchRole is an [AWS managed policy](#).

Using this policy

You can attach ServerMigrationServiceLaunchRole to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** November 26, 2018, 19:53 UTC
- **Edited time:** October 15, 2020, 17:29 UTC
- **ARN:** arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
      }
    }
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServerMigrationServiceRoleForInstanceValidation

Description: Permissions to allow the AWS SMS to run used data validation script and send script success/failure back to SMS

ServerMigrationServiceRoleForInstanceValidation is an [AWS managed policy](#).

Using this policy

You can attach ServerMigrationServiceRoleForInstanceValidation to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** July 20, 2020, 22:25 UTC
- **Edited time:** July 20, 2020, 22:25 UTC

- **ARN:** `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServiceQuotasFullAccess

Description: Provides full access to Service Quotas

ServiceQuotasFullAccess is an [AWS managed policy](#).

Using this policy

You can attach ServiceQuotasFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2019, 15:44 UTC
- **Edited time:** February 04, 2021, 21:29 UTC
- **ARN:** arn:aws:iam::aws:policy/ServiceQuotasFullAccess

Policy version

Policy version: v4 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  }
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServiceQuotasReadOnlyAccess

Description: Provides read only access to Service Quotas

ServiceQuotasReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach ServiceQuotasReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** June 24, 2019, 15:31 UTC
- **Edited time:** December 21, 2020, 18:11 UTC
- **ARN:** arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ServiceQuotasServiceRolePolicy

Description: Allows Service Quotas to create support cases on your behalf

ServiceQuotasServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** May 22, 2019, 20:44 UTC
- **Edited time:** June 24, 2019, 14:52 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SimpleWorkflowFullAccess

Description: Provides full access to the Simple Workflow configuration service.

SimpleWorkflowFullAccess is an [AWS managed policy](#).

Using this policy

You can attach SimpleWorkflowFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** February 06, 2015, 18:41 UTC
- **Edited time:** February 06, 2015, 18:41 UTC

- **ARN:** `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SplitCostAllocationDataServiceRolePolicy

Description: Allows split cost allocation data to retrieve AWS Organizations information, if applicable, and collect telemetry data for the split cost allocation data services that the customer has opted in to.

SplitCostAllocationDataServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** April 16, 2024, 16:05 UTC
- **Edited time:** April 16, 2024, 16:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SSMQuickSetupRolePolicy

Description: Provides permissions to check Quick Setup configuration health, ensure consistent use of parameters and provisioned resources, and remediate resources when drift is detected.

SSMQuickSetupRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** June 25, 2024, 15:20 UTC
- **Edited time:** June 25, 2024, 15:20 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
```



```

    "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
  ]
},
{
  "Sid" : "OrganizationReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListRoots",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAccountsForParent",
    "organizations:ListOrganizationalUnitsForParent"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QuickSetupStackSetReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
  ]
},
{
  "Sid" : "QuickSetupStackSetDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation>DeleteStackInstances",
    "cloudformation>DeleteStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
    "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
    "arn:aws:cloudformation:*:*:type/resource/*"
  ],
  "Condition" : {

```

```
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SupportUser

Description: This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.

SupportUser is an [AWS managed policy](#).

Using this policy

You can attach SupportUser to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:21 UTC
- **Edited time:** August 25, 2023, 18:40 UTC
- **ARN:** arn:aws:iam::aws:policy/job-function/SupportUser

Policy version

Policy version: v8 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
}

```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

SystemAdministrator

Description: Grants full access permissions necessary for resources required for application and development operations.

SystemAdministrator is an [AWS managed policy](#).

Using this policy

You can attach SystemAdministrator to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:23 UTC
- **Edited time:** August 24, 2020, 20:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Policy version

Policy version: v6 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
      ]
    }
  ]
}
```



```
"acm:Resend*",
"autoscaling:*",
"cloudtrail:DescribeTrails",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListPublicKeys",
"cloudtrail:ListTags",
"cloudtrail:LookupEvents",
"cloudtrail:StartLogging",
"cloudtrail:StopLogging",
"cloudwatch:*",
"codecommit:BatchGetRepositories",
"codecommit:CreateBranch",
"codecommit:CreateRepository",
"codecommit:Get*",
"codecommit:GitPull",
"codecommit:GitPush",
"codecommit:List*",
"codecommit:Put*",
"codecommit:Test*",
"codecommit:Update*",
"codedeploy:*",
"codepipeline:*",
"config:*",
"ds:*",
"ec2:Allocate*",
"ec2:AssignPrivateIpAddresses*",
"ec2:Associate*",
"ec2:Allocate*",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVpnGateway",
"ec2:Bundle*",
"ec2:Cancel*",
"ec2:Copy*",
"ec2:CreateCustomerGateway",
"ec2:CreateDhcpOptions",
"ec2:CreateFlowLogs",
"ec2:CreateImage",
"ec2:CreateInstanceExportTask",
"ec2:CreateInternetGateway",
"ec2:CreateKeyPair",
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:CreateNatGateway",
```

```
"ec2:CreateNetworkInterface",
"ec2:CreatePlacementGroup",
"ec2:CreateReservedInstancesListing",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateSpotDatafeedSubscription",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteKeyPair",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkInterface",
"ec2>DeletePlacementGroup",
"ec2>DeleteSnapshot",
"ec2>DeleteSpotDatafeedSubscription",
"ec2>DeleteSubnet",
"ec2>DeleteTags",
"ec2>DeleteVpc",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteVpnConnection",
"ec2>DeleteVpnConnectionRoute",
"ec2>DeleteVpnGateway",
"ec2:DeregisterImage",
"ec2:Describe*",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVolumeIO",
"ec2:EnableVpcClassicLinkDnsSupport",
```

```
"ec2:GetConsoleOutput",
"ec2:GetHostReservationPurchasePreview",
"ec2:GetLaunchTemplateData",
"ec2:GetPasswordData",
"ec2:Import*",
"ec2:Modify*",
"ec2:MonitorInstances",
"ec2:MoveAddressToVpc",
"ec2:Purchase*",
"ec2:RegisterImage",
"ec2:Release*",
"ec2:Replace*",
"ec2:ReportInstanceStatus",
"ec2:Request*",
"ec2:Reset*",
"ec2:RestoreAddressToClassic",
"ec2:RunScheduledInstances",
"ec2:UnassignPrivateIpAddresses",
"ec2:UnmonitorInstances",
"ec2:UpdateSecurityGroupRuleDescriptionsEgress",
"ec2:UpdateSecurityGroupRuleDescriptionsIngress",
"elasticloadbalancing:*",
"events:*",
"iam:GetAccount*",
"iam:GetContextKeys*",
"iam:GetCredentialReport",
"iam:ListAccountAliases",
"iam:ListGroups",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListPoliciesGrantingServiceAccess",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:Simulate*",
"iam:UpdateServerCertificate",
"iam:UpdateSigningCertificate",
"kinesis:ListStreams",
"kinesis:PutRecord",
"kms:CreateAlias",
"kms:CreateKey",
"kms>DeleteAlias",
"kms:Describe*",
"kms:GenerateRandom",
```

```
    "kms:Get*",
    "kms:List*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "lambda:Create*",
    "lambda:Delete*",
    "lambda:Get*",
    "lambda:InvokeFunction",
    "lambda:List*",
    "lambda:PublishVersion",
    "lambda:Update*",
    "logs:*",
    "rds:Describe*",
    "rds:ListTagsForResource",
    "route53:*",
    "route53domains:*",
    "ses:*",
    "sns:*",
    "sqs:*",
    "trustedadvisor:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "ec2:AcceptVpcPeeringConnection",
    "ec2:AttachClassicLinkVpc",
    "ec2:AttachVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateVpcPeeringConnection",
    "ec2>DeleteCustomerGateway",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteNetworkAcl*",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteVolume",
    "ec2>DeleteVpcPeeringConnection",
    "ec2:DetachClassicLinkVpc",
    "ec2:DetachVolume",
    "ec2:DisableVpcClassicLink",
```

```
    "ec2:EnableVpcClassicLink",
    "ec2:GetConsoleScreenshot",
    "ec2:RebootInstances",
    "ec2:RejectVpcPeeringConnection",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "s3:*",
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "iam:GetAccessKeyLastUsed",
    "iam:GetGroup*",
    "iam:GetInstanceProfile",
    "iam:GetLoginProfile",
    "iam:GetOpenIDConnectProvider",
    "iam:GetPolicy*",
    "iam:GetRole*",
    "iam:GetSAMLProvider",
    "iam:GetSSHPublicKey",
    "iam:GetServerCertificate",
    "iam:GetServiceLastAccessed*",
    "iam:GetUser*",
    "iam:ListAccessKeys",
    "iam:ListAttached*",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroupsForUser",
    "iam:ListInstanceProfiles*",
    "iam:ListMFADevices",
```

```
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "iam:ListSSHPublicKeys",
    "iam:ListSigningCertificates",
    "iam:ListUserPolicies",
    "iam:Upload*"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/rds-monitoring-role",
    "arn:aws:iam::*:role/ec2-sysadmin-*",
    "arn:aws:iam::*:role/ecr-sysadmin-*",
    "arn:aws:iam::*:role/lambda-sysadmin-*"
  ]
}
],
"Version" : "2012-10-17"
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

TranslateFullAccess

Description: Provides full access to Amazon Translate.

TranslateFullAccess is an [AWS managed policy](#).

Using this policy

You can attach TranslateFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 27, 2018, 23:36 UTC
- **Edited time:** January 08, 2020, 21:22 UTC
- **ARN:** `arn:aws:iam::aws:policy/TranslateFullAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
  }
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

TranslateReadOnly

Description: Provides read-only access to Amazon Translate.

TranslateReadOnly is an [AWS managed policy](#).

Using this policy

You can attach TranslateReadOnly to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2017, 18:22 UTC
- **Edited time:** May 24, 2023, 17:19 UTC
- **ARN:** arn:aws:iam::aws:policy/TranslateReadOnly

Policy version

Policy version: v7 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

ViewOnlyAccess

Description: This policy grants permissions to view resources and basic metadata across all AWS services.

ViewOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `ViewOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** Job function policy
- **Creation time:** November 10, 2016, 17:20 UTC
- **Edited time:** June 10, 2024, 20:57 UTC
- **ARN:** `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Policy version

Policy version: v19 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
```

```
"backup:DescribeReportJob",
"backup:DescribeReportPlan",
"backup:DescribeRestoreJob",
"backup:GetSupportedResourceTypes",
"backup:ListBackupJobs",
"backup:ListBackupPlanTemplates",
"backup:ListBackupPlanVersions",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListCopyJobs",
"backup:ListFrameworks",
"backup:ListLegalHolds",
"backup:ListProtectedResources",
"backup:ListProtectedResourcesByBackupVault",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListRecoveryPointsByLegalHold",
"backup:ListRecoveryPointsByResource",
"backup:ListReportJobs",
"backup:ListReportPlans",
"backup:ListRestoreJobs",
"backup:ListTags",
"batch:ListJobs",
"bedrock:ListCustomModels",
"bedrock:ListTagsForResource",
"clouddirectory:ListAppliedSchemaArns",
"clouddirectory:ListDevelopmentSchemaArns",
"clouddirectory:ListDirectories",
"clouddirectory:ListPublishedSchemaArns",
"cloudformation:DescribeStacks",
"cloudformation:List*",
"cloudfront:List*",
"cloudsearch:DescribeDomains",
"cloudsearch:List*",
"cloudtrail:DescribeTrails",
"cloudtrail:ListTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"codebuild:ListBuilds*",
"codebuild:ListProjects",
"codecommit:List*",
"codedeploy:BatchGetApplicationRevisions",
"codedeploy:BatchGetApplications",
```

```
"codedeploy:BatchGetDeploymentGroups",
"codedeploy:BatchGetDeploymentInstances",
"codedeploy:BatchGetDeploymentTargets",
"codedeploy:BatchGetDeployments",
"codedeploy:BatchGetOnPremisesInstances",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:ListPipelines",
"codestar:List*",
"cognito-identity:ListIdentities",
"cognito-identity:ListIdentityPools",
"cognito-idp:List*",
"cognito-sync:ListDatasets",
"comprehend:Describe*",
"comprehend:List*",
"config:Describe*",
"config:List*",
"connect:List*",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendationSummaries",
"cost-optimization-hub:ListRecommendations",
"databrew:ListJobs",
"databrew:ListProjects",
"datapipeline:DescribePipelines",
"datapipeline:GetAccountLimits",
"datapipeline:ListPipelines",
"dax:DescribeClusters",
"dax:DescribeDefaultParameters",
"dax:DescribeEvents",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"devicefarm:List*",
"directconnect:Describe*",
"discovery:List*",
"dms:List*",
"ds:DescribeDirectories",
"dynamodb:DescribeBackup",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
```

```
"dynamodb:DescribeLimits",
"dynamodb:DescribeReservedCapacity",
"dynamodb:DescribeReservedCapacityOfferings",
"dynamodb:DescribeStream",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListExports",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeBundleTasks",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeExportTasks",
"ec2:DescribeFlowLogs",
"ec2:DescribeHost*",
"ec2:DescribeIdFormat",
"ec2:DescribeIdentityIdFormat",
"ec2:DescribeImage*",
"ec2:DescribeImport*",
"ec2:DescribeInstance*",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeLocalGatewayRouteTables",
"ec2:DescribeLocalGatewayVirtualInterfaceGroups",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeLocalGateways",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetwork*",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeReserved*",
```

```
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshot*",
"ec2:DescribeSpot*",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolume*",
"ec2:DescribeVpc*",
"ec2:DescribeVpnGateways",
"ec2:SearchLocalGatewayRoutes",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"eks:ListTagsForResource",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:DescribeAccelerators",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeEnvironments",
"elasticbeanstalk:ListAvailableSolutionStacks",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:List*",
"elastictranscoder:List*",
"emr-serverless:ListApplications",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
"events:ListRuleNamesByTarget",
"events:ListRules",
"events:ListTargetsByRule",
"firehose:DescribeDeliveryStream",
"firehose:List*",
"fsx:DescribeFileSystems",
```

```
"gamelift:List*",
"glacier:List*",
"glue:GetTags",
"greengrass:List*",
"iam:GetAccountSummary",
"iam:GetLoginProfile",
"iam:List*",
"importexport:ListJobs",
"inspector:List*",
"iot:List*",
"kafka:ListClusters",
"kendra:ListDataSources",
"kendra:ListTagsForResource",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kms:ListKeys",
"kms:ListResourceTags",
"lambda:List*",
"lex:GetBotAliases",
"lex:GetBotChannelAssociations",
"lex:GetBotVersions",
"lex:GetBots",
"lex:GetIntentVersions",
"lex:GetIntents",
"lex:GetSlotTypeVersions",
"lex:GetSlotTypes",
"lex:GetUtterancesView",
"lightsail:GetBlueprints",
"lightsail:GetBundles",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetRegions",
"lightsail:GetStaticIps",
"lightsail:IsVpcPeered",
"logs:Describe*",
"logs:ListTagsForResource",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"machinelearning:Describe*",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
```

```
"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"
]
}
]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

VMImportExportRoleForAWSConnector

Description: Default policy for the VM Import/Export service role, for customers using the AWS Connector. The VM Import/Export service assumes a role with this policy to fulfill virtual machine migration requests from the AWS Connector virtual appliance. (Note that the AWS Connector uses the "AWSConnector" managed policy to issue requests on the customer's behalf to the VM Import/Export service.) Provides the ability to create AMIs and EBS snapshots, modify EBS snapshot attributes, make "Describe*" calls on EC2 objects, and read from S3 buckets starting with 'import-to-ec2-'.

VMImportExportRoleForAWSConnector is an [AWS managed policy](#).

Using this policy

You can attach VMImportExportRoleForAWSConnector to your users, groups, and roles.

Policy details

- **Type:** Service role policy
- **Creation time:** September 03, 2015, 20:48 UTC
- **Edited time:** September 03, 2015, 20:48 UTC
- **ARN:** `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

VPCLatticeFullAccess

Description: Provides full access to Amazon VPC Lattice and access to dependency services.

VPCLatticeFullAccess is an [AWS managed policy](#).

Using this policy

You can attach VPCLatticeFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 30, 2023, 02:49 UTC
- **Edited time:** March 30, 2023, 02:49 UTC
- **ARN:** arn:aws:iam::aws:policy/VPCLatticeFullAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

VPCLatticeReadOnlyAccess

Description: Provides read-only access to Amazon VPC Lattice via the AWS Management Console, and limited access to dependency services.

VPCLatticeReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach `VPCLatticeReadOnlyAccess` to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 30, 2023, 02:47 UTC
- **Edited time:** March 30, 2023, 02:47 UTC
- **ARN:** `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
}
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

VPCLatticeServicesInvokeAccess

Description: Provides access to invoking Amazon VPC Lattice services.

VPCLatticeServicesInvokeAccess is an [AWS managed policy](#).

Using this policy

You can attach VPCLatticeServicesInvokeAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** March 30, 2023, 02:45 UTC
- **Edited time:** March 30, 2023, 02:45 UTC
- **ARN:** arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WAFLoggingServiceRolePolicy

Description: Creating SLR to write customer's logs to a firehose stream

WAFLoggingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 24, 2018, 21:05 UTC
- **Edited time:** August 24, 2018, 21:05 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WAFRegionalLoggingServiceRolePolicy

Description: Creating SLR to write customer's logs to a firehose stream

WAFRegionalLoggingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** August 24, 2018, 18:40 UTC
- **Edited time:** August 24, 2018, 18:40 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{  
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
    ]
  }
]
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WAFV2LoggingServiceRolePolicy

Description: This policy creates a service-linked role that allows AWS WAF to write logs to Amazon Kinesis Data Firehose.

WAFV2LoggingServiceRolePolicy is an [AWS managed policy](#).

Using this policy

This policy is attached to a service-linked role that allows the service to perform actions on your behalf. You cannot attach this policy to your users, groups, or roles.

Policy details

- **Type:** Service-linked role policy
- **Creation time:** November 07, 2019, 00:40 UTC
- **Edited time:** June 03, 2024, 17:29 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Policy version

Policy version: v3 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Learn more

- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WellArchitectedConsoleFullAccess

Description: Provides full access to AWS Well-Architected Tool via the AWS Management Console

WellArchitectedConsoleFullAccess is an [AWS managed policy](#).

Using this policy

You can attach WellArchitectedConsoleFullAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2018, 18:19 UTC
- **Edited time:** November 29, 2018, 18:19 UTC
- **ARN:** `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WellArchitectedConsoleReadOnlyAccess

Description: Provides read-only access to AWS Well-Architected Tool via the AWS Management Console

WellArchitectedConsoleReadOnlyAccess is an [AWS managed policy](#).

Using this policy

You can attach WellArchitectedConsoleReadOnlyAccess to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** November 29, 2018, 18:21 UTC
- **Edited time:** June 29, 2023, 17:16 UTC
- **ARN:** `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Policy version

Policy version: v2 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "wellarchitected:Get*",
      "wellarchitected:List*",
      "wellarchitected:ExportLens"
    ],
    "Resource" : "*"
  }
]
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)

WorkLinkServiceRolePolicy

Description: Enables access to AWS services and Resources used or managed by Amazon WorkLink

WorkLinkServiceRolePolicy is an [AWS managed policy](#).

Using this policy

You can attach WorkLinkServiceRolePolicy to your users, groups, and roles.

Policy details

- **Type:** AWS managed policy
- **Creation time:** January 23, 2019, 19:03 UTC
- **Edited time:** January 23, 2019, 19:03 UTC
- **ARN:** arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

Policy version

Policy version: v1 (default)

The policy's default version is the version that defines the permissions for the policy. When a user or role with the policy makes a request to access an AWS resource, AWS checks the default version of the policy to determine whether to allow the request.

JSON policy document

```
{
  "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-*"
    }
  ]
}
```

Learn more

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [Adding and removing IAM identity permissions](#)
- [Understand versioning for IAM policies](#)
- [Get started with AWS managed policies and move toward least-privilege permissions](#)