



Guide de référence

AWS Politique gérée



AWS Politique gérée: Guide de référence

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Que sont les politiques AWS gérées ?	1
Comprendre les pages de référence des politiques	1
Politiques gérées par AWS obsolètes	2
AWS politiques gérées	3
AccessAnalyzerServiceRolePolicy	43
Utilisation de cette politique	43
Détails de la politique	43
Version de la politique	43
Document de politique JSON	44
En savoir plus	46
AdministratorAccess	46
Utilisation de cette politique	46
Détails de la politique	46
Version de la politique	46
Document de politique JSON	47
En savoir plus	47
AdministratorAccess-Amplify	47
Utilisation de cette stratégie	47
Détails des politiques	47
Version de la politique	48
Document de stratégie JSON	48
En savoir plus	58
AdministratorAccess-AWSElasticBeanstalk	58
Utilisation de cette stratégie	58
Détails de la stratégie	59
Version de la politique	59
Document de stratégie JSON	59
En savoir plus	67
AlexaForBusinessDeviceSetup	67
Utilisation de cette stratégie	68
Détails des politiques	68
Version de la politique	68
Document de stratégie JSON	68
En savoir plus	69

AlexaForBusinessFullAccess	69
Utilisation de cette stratégie	69
Détails des politiques	69
Version de la politique	69
Document de stratégie JSON	70
En savoir plus	71
AlexaForBusinessGatewayExecution	71
Utilisation de cette stratégie	71
Détails des politiques	71
Version de la politique	72
Document de stratégie JSON	72
En savoir plus	73
AlexaForBusinessLifesizeDelegatedAccessPolicy	73
Utilisation de la présente stratégie	73
Détails des politiques	73
Version de la politique	73
Document de stratégie JSON	74
En savoir plus	76
AlexaForBusinessNetworkProfileServicePolicy	76
Utilisation cette politique en utilisant cette politique	76
Les détails des politiques politiques	76
Version de la politique	77
Document de stratégie JSON document de	77
En savoir plus	78
AlexaForBusinessPolyDelegatedAccessPolicy	78
Utilisation de cette stratégie	78
Détails des politiques	78
Version de la politique	78
Document de stratégie JSON	78
En savoir plus	80
AlexaForBusinessReadOnlyAccess	80
Utilisation de cette stratégie	80
Détails des politiques	81
Version de la politique	81
Document de stratégie JSON	81
En savoir plus	81

AmazonAPIGatewayAdministrator	82
Utilisation de cette stratégie	82
Détails des politiques	82
Version de la politique	82
Document de stratégie JSON	82
En savoir plus	83
AmazonAPIGatewayInvokeFullAccess	83
Utilisation de cette stratégie	83
Détails des politiques	83
Version de la politique	83
Document de stratégie JSON	84
En savoir plus	84
AmazonAPIGatewayPushToCloudWatchLogs	84
Utilisation de cette stratégie	84
Détails des politiques	84
Version de la politique	85
Document de stratégie JSON	85
En savoir plus	85
AmazonAppFlowFullAccess	86
Utilisation de cette stratégie	86
Détails des politiques	86
Version de la politique	86
Document de stratégie JSON	86
En savoir plus	89
AmazonAppFlowReadOnlyAccess	89
Utilisation de cette stratégie	89
Détails des politiques	89
Version de la politique	90
Document de stratégie JSON	90
En savoir plus	90
AmazonAppStreamFullAccess	91
Utilisation de cette stratégie	91
Détails des politiques	91
Version de la politique	91
Document de stratégie JSON	91
En savoir plus	93

AmazonAppStreamPCAAccess	93
Utilisation de cette stratégie	93
Détails des politiques	93
Version de la politique	94
Document de stratégie JSON	94
En savoir plus	94
AmazonAppStreamReadOnlyAccess	95
Utilisation de cette stratégie	95
Détails des politiques	95
Version de la politique	95
Document de stratégie JSON	95
En savoir plus	96
AmazonAppStreamServiceAccess	96
Utilisation de cette stratégie	96
Détails des politiques	96
Version de la politique	96
Document de stratégie JSON	96
En savoir plus	98
AmazonAthenaFullAccess	98
Utilisation de cette politique	98
Détails de la politique	98
Version de la politique	98
Document de politique JSON	98
En savoir plus	102
AmazonAugmentedAIFullAccess	102
Utilisation de cette stratégie	102
Détails des politiques	102
Version de la politique	102
Document de stratégie JSON	103
En savoir plus	104
AmazonAugmentedAIHumanLoopFullAccess	104
Utilisation de cette stratégie	104
Détails des politiques	104
Version de la politique	104
Document de stratégie JSON	105
En savoir plus	105

AmazonAugmentedAllIntegratedAPIAccess	105
Utilisation de cette stratégie	105
Détails des politiques	105
Version de la politique	106
Document de stratégie JSON	106
En savoir plus	107
AmazonBedrockFullAccess	107
Utilisation de cette politique	108
Détails de la politique	108
Version de la politique	108
Document de politique JSON	108
En savoir plus	109
AmazonBedrockReadOnly	109
Utilisation de cette politique	110
Détails de la politique	110
Version de la politique	110
Document de politique JSON	110
En savoir plus	111
AmazonBraketFullAccess	111
Utilisation de cette stratégie	111
Détails des politiques	111
Version de la politique	111
Document de stratégie JSON	112
En savoir plus	116
AmazonBraketJobsExecutionPolicy	116
Utilisation de cette stratégie	116
Détails des politiques	116
Version de la politique	116
Document de stratégie JSON	117
En savoir plus	119
AmazonBraketServiceRolePolicy	119
Utilisation des stratégies de politique	119
Les politiques	120
Version de la politique	120
Document de stratégie JSON	120
En savoir plus	121

AmazonChimeFullAccess	121
Utilisation de cette stratégie	121
Détails des politiques	121
Version de la politique	121
Document de stratégie JSON	121
En savoir plus	123
AmazonChimeReadOnly	124
Utilisation de cette stratégie	124
Détails des politiques	124
Version de la politique	124
Document de stratégie JSON	124
En savoir plus	125
AmazonChimeSDK	125
Utilisation de cette stratégie	125
Détails des politiques	125
Version de la politique	125
Document de stratégie JSON	126
En savoir plus	127
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	127
Utilisation de cette politique	127
Détails de la politique	127
Version de la politique	127
Document de politique JSON	128
En savoir plus	129
AmazonChimeSDKMessagingServiceRolePolicy	129
Utilisation des politique de politique de politique	129
les politique de politique	129
Version de la politique	129
politique JSON	130
En savoir plus	130
AmazonChimeServiceRolePolicy	131
Utilisation de cette politique	131
Les détails des politiques	131
Version de la politique	131
Document de stratégie JSON	131
En savoir plus	132

AmazonChimeTranscriptionServiceLinkedRolePolicy	132
Using this policy	132
Policy details	132
Version de la politique	132
JSON policy document	133
En savoir plus	133
AmazonChimeUserManagement	133
Utilisation de cette stratégie	133
Détails des politiques	133
Version de la politique	134
Document de stratégie JSON	134
En savoir plus	135
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	135
Utilisation de cette politique	135
Les détails des politiques	135
Version de la politique	136
Document de stratégie JSON	136
En savoir plus	138
AmazonCloudDirectoryFullAccess	138
Utilisation de cette stratégie	138
Détails des politiques	138
Version de la politique	138
Document de stratégie JSON	138
En savoir plus	139
AmazonCloudDirectoryReadOnlyAccess	139
Utilisation de cette stratégie	139
Détails des politiques	139
Version de la politique	140
Document de stratégie JSON	140
En savoir plus	140
AmazonCloudWatchEvidentlyFullAccess	141
Utilisation de cette stratégie	141
Détails des politiques	141
Version de la politique	141
Document de stratégie JSON	141
En savoir plus	144

AmazonCloudWatchEvidentlyReadOnlyAccess	144
Utilisation de cette stratégie	144
Détails des politiques	144
Version de la politique	144
Document de stratégie JSON	145
En savoir plus	145
AmazonCloudWatchEvidentlyServiceRolePolicy	145
Utilisation de cette politique	145
Les détails des politiques	146
Version de la politique	146
Document de stratégie JSON	146
En savoir plus	147
AmazonCloudWatchRUMFullAccess	148
Utilisation de cette stratégie	148
Détails des politiques	148
Version de la politique	148
Document de stratégie JSON	148
En savoir plus	151
AmazonCloudWatchRUMReadOnlyAccess	151
Utilisation de cette stratégie	151
Détails des politiques	151
Version de la politique	151
Document de stratégie JSON	151
En savoir plus	152
AmazonCloudWatchRUMServiceRolePolicy	152
Utilisation des des des des des politiques	152
Détails des des des politiques	152
Version de la politique	153
Document de de de stratégie JAM	153
En savoir plus	154
AmazonCodeCatalystFullAccess	154
Utilisation de cette stratégie	154
Détails des politiques	154
Version de la politique	154
Document de stratégie JSON	154
En savoir plus	155

AmazonCodeCatalystReadOnlyAccess	155
Utilisation de cette stratégie	156
Détails des politiques	156
Version de la politique	156
Document de stratégie JSON	156
En savoir plus	156
AmazonCodeCatalystSupportAccess	157
Utilisation de cette stratégie	157
Détails des politiques	157
Version de la politique	157
Document de stratégie JSON	157
En savoir plus	158
AmazonCodeGuruProfilerAgentAccess	158
Utilisation de cette stratégie	158
Détails des politiques	159
Version de la politique	159
Document de stratégie JSON	159
En savoir plus	159
AmazonCodeGuruProfilerFullAccess	160
Utilisation de cette stratégie	160
Détails des politiques	160
Version de la politique	160
Document de stratégie JSON	160
En savoir plus	161
AmazonCodeGuruProfilerReadOnlyAccess	161
Utilisation de cette stratégie	161
Détails des politiques	161
Version de la politique	162
Document de stratégie JSON	162
En savoir plus	162
AmazonCodeGuruReviewerFullAccess	163
Utilisation de cette stratégie	163
Détails des politiques	163
Version de la politique	163
Document de stratégie JSON	163
En savoir plus	166

AmazonCodeGuruReviewerReadOnlyAccess	166
Utilisation de cette stratégie	166
Détails des politiques	166
Version de la politique	166
Document de stratégie JSON	167
En savoir plus	167
AmazonCodeGuruReviewerServiceRolePolicy	167
Utilisation de cette politique politique politique	168
Les politiques	168
Version de la politique	168
Document politique JSON Document de politique	168
En savoir plus	170
AmazonCodeGuruSecurityFullAccess	170
Utilisation de cette stratégie	170
Détails des politiques	171
Version de la politique	171
Document de stratégie JSON	171
En savoir plus	171
AmazonCodeGuruSecurityScanAccess	172
Utilisation de cette stratégie	172
Détails des politiques	172
Version de la politique	172
Document de stratégie JSON	172
En savoir plus	173
AmazonCognitoDeveloperAuthenticatedIdentities	173
Utilisation de cette stratégie	173
Détails des politiques	173
Version de la politique	173
Document de stratégie JSON	174
En savoir plus	174
AmazonCognitoIdpEmailServiceRolePolicy	174
Utilisation politique Utilisation cette politique ISON	174
détails politiques IAM	175
Version de la politique	175
Document politique JSON	175
En savoir plus	176

AmazonCognitoIkpServiceRolePolicy	176
Utilisation	176
Les politiques	176
Version de la politique	176
Document	176
En savoir plus	177
AmazonCognitoPowerUser	177
Utilisation de cette stratégie	177
Détails des politiques	177
Version de la politique	177
Document de stratégie JSON	178
En savoir plus	179
AmazonCognitoReadOnly	179
Utilisation de cette stratégie	179
Détails des politiques	179
Version de la politique	180
Document de stratégie JSON	180
En savoir plus	180
AmazonCognitoUnAuthedIdentitiesSessionPolicy	181
Utilisation de cette politique	181
Détails de la politique	181
Version de la politique	181
Document de politique JSON	182
En savoir plus	182
AmazonCognitoUnauthenticatedIdentities	182
Utilisation de cette stratégie	183
Détails des politiques	183
Version de la politique	183
Document de stratégie JSON	183
En savoir plus	183
AmazonConnect_FullAccess	184
Utilisation de cette politique	184
Détails de la politique	184
Version de la politique	184
Document de stratégie JSON	184
En savoir plus	187

AmazonConnectCampaignsServiceLinkedRolePolicy	187
Utilisation de cette politique	187
Détails de la politique	187
Version de la politique	188
Document de politique JSON	188
En savoir plus	188
AmazonConnectReadOnlyAccess	189
Utilisation de cette stratégie	189
Détails des politiques	189
Version de la politique	189
Document de stratégie JSON	189
En savoir plus	190
AmazonConnectServiceLinkedRolePolicy	190
Utilisation de cette politique	190
Détails de la politique	190
Version de la politique	190
Document de politique JSON	191
En savoir plus	195
AmazonConnectSynchronizationServiceRolePolicy	195
Utilisation de cette politique	196
Détails de la politique	196
Version de la politique	196
Document de politique JSON	196
En savoir plus	198
AmazonConnectVoiceIDFullAccess	198
Utilisation de cette stratégie	198
Détails des politiques	198
Version de la politique	199
Document de stratégie JSON	199
En savoir plus	199
AmazonDataZoneDomainExecutionRolePolicy	199
Utilisation de cette politique	200
Détails de la politique	200
Version de la politique	200
Document de politique JSON	200
En savoir plus	203

AmazonDataZoneEnvironmentRolePermissionsBoundary	203
Utilisation de cette politique	203
Détails de la politique	203
Version de la politique	204
Document de politique JSON	204
En savoir plus	217
AmazonDataZoneFullAccess	217
Utilisation de cette politique	217
Détails de la politique	217
Version de la politique	217
Document de politique JSON	217
En savoir plus	221
AmazonDataZoneFullUserAccess	221
Utilisation de cette politique	221
Détails de la politique	221
Version de la politique	221
Document de politique JSON	222
En savoir plus	224
AmazonDataZoneGlueManageAccessRolePolicy	225
Utilisation de cette politique	225
Détails de la politique	225
Version de la politique	225
Document de politique JSON	225
En savoir plus	229
AmazonDataZonePortalFullAccessPolicy	229
Utilisation de cette stratégie	229
Détails des politiques	229
Version de la politique	229
Document de stratégie JSON	230
En savoir plus	230
AmazonDataZonePreviewConsoleFullAccess	230
Utilisation de cette politique	230
Détails de la politique	230
Version de la politique	231
Document de politique JSON	231
En savoir plus	233

AmazonDataZoneProjectDeploymentPermissionsBoundary	233
Utilisation de cette stratégie	233
Détails des politiques	233
Version de la politique	233
Document de stratégie JSON	234
En savoir plus	242
AmazonDataZoneProjectRolePermissionsBoundary	242
Utilisation de cette stratégie	242
Détails des politiques	242
Version de la politique	242
Document de stratégie JSON	243
En savoir plus	250
AmazonDataZoneRedshiftGlueProvisioningPolicy	250
Utilisation de cette politique	250
Détails de la politique	250
Version de la politique	250
Document de politique JSON	251
En savoir plus	258
AmazonDataZoneRedshiftManageAccessRolePolicy	259
Utilisation de cette politique	259
Détails de la politique	259
Version de la politique	259
Document de politique JSON	259
En savoir plus	261
AmazonDetectiveFullAccess	262
Utilisation de cette stratégie	262
Détails de politiques	262
Version de la politique	262
Document de stratégie JSON	262
En savoir plus	263
AmazonDetectiveInvestigatorAccess	263
Utilisation de cette politique	264
Détails de la politique	264
Version de la politique	264
Document de politique JSON	264
En savoir plus	266

AmazonDetectiveMemberAccess	266
Utilisation de cette stratégie	266
Détails des politiques	266
Version de la politique	266
Document de stratégie JSON	266
En savoir plus	267
AmazonDetectiveOrganizationsAccess	267
Utilisation de cette stratégie	267
Détails des politiques	267
Version de la politique	268
Document de stratégie JSON	268
En savoir plus	270
AmazonDetectiveServiceLinkedRolePolicy	270
des politiques de politique de stratégie politique	270
Les politiques politiques de politique	270
Version de la politique	270
Document de stratégie JSON	270
En savoir plus	271
AmazonDevOpsGuruConsoleFullAccess	271
Utilisation de cette stratégie	271
Détails des politiques	271
Version de la politique	272
Document de stratégie JSON	272
En savoir plus	274
AmazonDevOpsGuruFullAccess	274
Utilisation de cette stratégie	274
Détails des politiques	275
Version de la politique	275
Document de stratégie JSON	275
En savoir plus	277
AmazonDevOpsGuruOrganizationsAccess	277
Utilisation de cette stratégie	278
Détails des politiques	278
Version de la politique	278
Document de stratégie JSON	278
En savoir plus	279

AmazonDevOpsGuruReadOnlyAccess	280
Utilisation de cette stratégie	280
Détails des politiques	280
Version de la politique	280
Document de stratégie JSON	280
En savoir plus	282
AmazonDevOpsGuruServiceRolePolicy	282
Utilisation de cette politique	282
Les détails des politiques	283
Version de la politique	283
Document de stratégie JSON	283
En savoir plus	287
AmazonDMSCloudWatchLogsRole	287
Utilisation de cette stratégie	287
Détails des politiques	287
Version de la politique	288
Document de stratégie JSON	288
En savoir plus	289
AmazonDMSRedshiftS3Role	289
Utilisation de cette stratégie	290
Détails des politiques	290
Version de la politique	290
Document de stratégie JSON	290
En savoir plus	291
AmazonDMSVPCManagementRole	291
Utilisation de cette stratégie	291
Détails des politiques	291
Version de la politique	291
Document de stratégie JSON	292
En savoir plus	292
AmazonDocDB-ElasticServiceRolePolicy	292
Utilisation de cette politique	293
Obtenir les détails des politiques	293
Version de la politique	293
Document de stratégie JSON	293
En savoir plus	294

AmazonDocDBConsoleFullAccess	294
Utilisation de cette stratégie	294
Détails des politiques	294
Version de la politique	294
Document de stratégie JSON	295
En savoir plus	299
AmazonDocDBElasticFullAccess	299
Utilisation de cette politique	299
Détails de la politique	299
Version de la politique	299
Document de politique JSON	300
En savoir plus	303
AmazonDocDBElasticReadOnlyAccess	303
Utilisation de cette politique	303
Détails de la politique	303
Version de la politique	303
Document de politique JSON	303
En savoir plus	304
AmazonDocDBFullAccess	304
Utilisation de cette stratégie	304
Détails des politiques	305
Version de la politique	305
Document de stratégie JSON	305
En savoir plus	308
AmazonDocDBReadOnlyAccess	308
Utilisation de cette stratégie	308
Détails des politiques	308
Version de la politique	308
Document de stratégie JSON	308
En savoir plus	310
AmazonDRSVPCManagement	310
Utilisation de cette stratégie	311
Détails des politiques	311
Version de la politique	311
Document de stratégie JSON	311
En savoir plus	312

AmazonDynamoDBFullAccess	312
Utilisation de cette stratégie	312
Détails des politiques	312
Version de la politique	312
Document de stratégie JSON	313
En savoir plus	315
AmazonDynamoDBFullAccesswithDataPipeline	315
Utilisation de cette stratégie	316
Détails des politiques	316
Version de la politique	316
Document de stratégie JSON	316
En savoir plus	318
AmazonDynamoDBReadOnlyAccess	318
Utilisation de cette politique	318
Détails de la politique	319
Version de la politique	319
Document de politique JSON	319
En savoir plus	321
AmazonEBSCSIDriverPolicy	321
Utilisation de cette politique	321
Détails des politiques	321
Version de la politique	321
Document de stratégie JSON	321
En savoir plus	325
AmazonEC2ContainerRegistryFullAccess	325
Utilisation de cette stratégie	325
Détails des politiques	325
Version de la politique	325
Document de stratégie JSON	325
En savoir plus	326
AmazonEC2ContainerRegistryPowerUser	326
Utilisation de cette stratégie	327
Détails des politiques	327
Version de la politique	327
Document de stratégie JSON	327
En savoir plus	328

AmazonEC2ContainerRegistryReadOnly	328
Utilisation de cette stratégie	328
Détails des politiques	328
Version de la politique	328
Document de stratégie JSON	329
En savoir plus	329
AmazonEC2ContainerServiceAutoscaleRole	330
Utilisation de cette stratégie	330
Détails des politiques	330
Version de la politique	330
Document de stratégie JSON	330
En savoir plus	331
AmazonEC2ContainerServiceEventsRole	331
Utilisation de cette stratégie	331
Détails des politiques	331
Version de la politique	332
Document de stratégie JSON	332
En savoir plus	333
AmazonEC2ContainerServiceforEC2Role	333
Utilisation de cette stratégie	333
Détails des politiques	333
Version de la politique	334
Document de stratégie JSON	334
En savoir plus	335
AmazonEC2ContainerServiceRole	335
Utilisation de cette stratégie	335
Détails des politiques	335
Version de la politique	335
Document de stratégie JSON	336
En savoir plus	336
AmazonEC2FullAccess	336
Utilisation de cette stratégie	337
Détails des politiques	337
Version de la politique	337
Document de stratégie JSON	337
En savoir plus	338

AmazonEC2ReadOnlyAccess	338
Utilisation de cette politique	338
Détails de la politique	339
Version de la politique	339
Document de politique JSON	339
En savoir plus	340
AmazonEC2RoleforAWSCodeDeploy	340
Utilisation de cette stratégie	340
Détails des politiques	340
Version de la politique	340
Document de stratégie JSON	341
En savoir plus	341
AmazonEC2RoleforAWSCodeDeployLimited	341
Utilisation de cette stratégie	341
Détails des politiques	342
Version de la politique	342
Document de stratégie JSON	342
En savoir plus	343
AmazonEC2RoleforDataPipelineRole	343
Utilisation de cette stratégie	343
Détails des politiques	343
Version de la politique	343
Document de stratégie JSON	344
En savoir plus	344
AmazonEC2RoleforSSM	345
Utilisation de cette politique	345
Détails des politiques	345
Version de la politique	345
Document de stratégie JSON	345
En savoir plus	347
AmazonEC2RolePolicyForLaunchWizard	348
Utilisation de cette stratégie	348
Détails des politiques	348
Version de la politique	348
Document de stratégie JSON	348
En savoir plus	352

AmazonEC2SpotFleetAutoscaleRole	352
Utilisation de cette stratégie	353
Détails des politiques	353
Version de la politique	353
Document de stratégie JSON	353
En savoir plus	354
AmazonEC2SpotFleetTaggingRole	354
Utilisation de cette stratégie	354
Détails des politiques	354
Version de la politique	355
Document de stratégie JSON	355
En savoir plus	356
AmazonECS_FullAccess	356
Utilisation de cette stratégie	357
Détails des politiques	357
Version de la politique	357
Document de stratégie JSON	357
En savoir plus	362
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	363
Utilisation de cette politique	363
Détails de la politique	363
Version de la politique	363
Document de politique JSON	363
En savoir plus	365
AmazonECSInfrastructureRolePolicyForVolumes	366
Utilisation de cette politique	366
Détails de la politique	366
Version de la politique	366
Document de politique JSON	366
En savoir plus	368
AmazonECSServiceRolePolicy	369
Utilisation de cette politique	369
Détails de la politique	369
Version de la politique	369
Document de politique JSON	369
En savoir plus	374

AmazonECSTaskExecutionRolePolicy	374
Utilisation de cette politique	374
Détails des politiques	374
Version de la politique	375
Document de politique JSON	375
En savoir plus	375
AmazonEFSCSIDriverPolicy	375
Utilisation de cette politique	376
Détails de la politique	376
Version de la politique	376
Document de politique JSON	376
En savoir plus	378
AmazonEKS_CNI_Policy	378
Utilisation de cette politique	378
Détails de la politique	378
Version de la politique	378
Document de politique JSON	379
En savoir plus	379
AmazonEKSClusterPolicy	380
Utilisation de cette stratégie	380
Détails des politiques	380
Version de la politique	380
Document de stratégie JSON	380
En savoir plus	382
AmazonEKSClusterServiceRolePolicy	383
Utilisation de cette politique	383
Les détails des politiques	383
Version de la politique	383
Document de stratégie JSON	383
En savoir plus	385
AmazonEKSFargatePodExecutionRolePolicy	385
Utilisation de cette politique	385
Détails des politiques	385
Version de la politique	386
Document de stratégie JSON	386
En savoir plus	386

AmazonEKSFargateServiceRolePolicy	387
Utilisation des des de de de de	387
Les détails des des des	387
Version de la politique	387
Document de de de de de de	387
En savoir plus	388
AmazonEKSLocalOutpostClusterPolicy	388
Utilisation de cette stratégie	388
Détails des politiques	388
Version de la politique	388
Document de stratégie JSON	389
En savoir plus	390
AmazonEKSLocalOutpostServiceRolePolicy	391
La politique de cette politique de politique	391
détails des politiques politiques politiques	391
Version de la politique	391
politique JSON de politique JSON	391
En savoir plus	397
AmazonEKSServicePolicy	397
Utilisation de cette politique	397
Détails des politiques	397
Version de la politique	398
Document de stratégie JSON	398
En savoir plus	399
AmazonEKSServiceRolePolicy	400
Utilisation de cette politique	400
Détails des politiques	400
Version de la politique	400
Document de stratégie JSON	400
En savoir plus	402
AmazonEKSVPCResourceController	403
Utilisation de cette stratégie	403
Détails des politiques	403
Version de la politique	403
Document de politique JSON	403
En savoir plus	404

AmazonEKSElasticContainerRegistryPublicFullAccess	404
Utilisation de cette politique	404
Détails de la politique	404
Version de la politique	405
Document de politique JSON	405
En savoir plus	405
AmazonEKSElasticContainerRegistryPublicPowerUser	406
Utilisation de cette politique	406
Détails de la politique	406
Version de la politique	406
Document de politique JSON	406
En savoir plus	409
AmazonEKSElasticContainerRegistryPublicReadOnly	410
Utilisation de cette stratégie	410
Détails des politiques	410
Version de la politique	410
Document de stratégie JSON	410
En savoir plus	411
AmazonEKSElasticContainerRegistryPublicFullAccess	411
Utilisation de cette stratégie	411
Détails des politiques	411
Version de la politique	411
Document de stratégie JSON	412
En savoir plus	412
AmazonEKSElasticContainerRegistryPublicPowerUser	412
Utilisation de cette stratégie	412
Détails des politiques	412
Version de la politique	413
Document de stratégie JSON	413
En savoir plus	414
AmazonEKSElasticContainerRegistryPublicReadOnly	414
Utilisation de cette stratégie	414
Détails des politiques	414
Version de la politique	414
Document de stratégie JSON	414
En savoir plus	415

AmazonElasticFileSystemClientFullAccess	415
Utilisation de cette stratégie	415
Détails des politiques	415
Version de la politique	416
Document de stratégie JSON	416
En savoir plus	416
AmazonElasticFileSystemClientReadOnlyAccess	417
Utilisation de cette stratégie	417
Détails des politiques	417
Version de la politique	417
Document de stratégie JSON	417
En savoir plus	418
AmazonElasticFileSystemClientReadWriteAccess	418
Utilisation de cette stratégie	418
Détails des politiques	418
Version de la politique	418
Document de stratégie JSON	418
En savoir plus	419
AmazonElasticFileSystemFullAccess	419
Utilisation de cette politique	419
Détails de la politique	419
Version de la politique	420
Document de politique JSON	420
En savoir plus	421
AmazonElasticFileSystemReadOnlyAccess	422
Utilisation de cette stratégie	422
Détails des politiques	422
Version de la politique	422
Document de stratégie JSON	422
En savoir plus	423
AmazonElasticFileSystemServiceRolePolicy	423
Utilisation de cette politique	424
Les détails des politiques	424
Version de la politique	424
Document de stratégie JSON	424
En savoir plus	426

AmazonElasticFileSystemsUtils	426
Utilisation de cette stratégie	426
Détails des politiques	427
Version de la politique	427
Document de stratégie JSON	427
En savoir plus	429
AmazonElasticMapReduceEditorsRole	429
Utilisation de cette stratégie	429
Détails de la stratégie	429
Version de la politique	429
Document de stratégie JSON	430
En savoir plus	431
AmazonElasticMapReduceforAutoScalingRole	431
Utilisation de cette stratégie	431
Détails des politiques	431
Version de la politique	431
Document de stratégie JSON	432
En savoir plus	432
AmazonElasticMapReduceforEC2Role	432
Utilisation de cette stratégie	432
Détails des politiques	433
Version de la politique	433
Document de stratégie JSON	433
En savoir plus	434
AmazonElasticMapReduceFullAccess	435
Utilisation de cette stratégie	435
Détails des politiques	435
Version de la politique	435
Document de stratégie JSON	435
En savoir plus	437
AmazonElasticMapReducePlacementGroupPolicy	437
Utilisation de cette stratégie	437
Détails des politiques	437
Version de la politique	438
Document de stratégie JSON	438
En savoir plus	438

AmazonElasticMapReduceReadOnlyAccess	439
Utilisation de cette stratégie	439
Détails des politiques	439
Version de la politique	439
Document de stratégie JSON	439
En savoir plus	440
AmazonElasticMapReduceRole	440
Utilisation de cette stratégie	440
Détails des politiques	440
Version de la politique	440
Document de stratégie JSON	441
En savoir plus	443
AmazonElasticsearchServiceRolePolicy	443
Utilisation de cette politique	443
Détails de la politique	443
Version de la politique	443
Document de politique JSON	444
En savoir plus	446
AmazonElasticTranscoder_FullAccess	447
Utilisation de cette stratégie	447
Détails des politiques	447
Version de la politique	447
Document de stratégie JSON	447
En savoir plus	448
AmazonElasticTranscoder_JobsSubmitter	448
Utilisation de cette stratégie	448
Détails des politiques	449
Version de la politique	449
Document de stratégie JSON	449
En savoir plus	449
AmazonElasticTranscoder_ReadOnlyAccess	450
Utilisation de cette stratégie	450
Détails des politiques	450
Version de la politique	450
Document de stratégie JSON	450
En savoir plus	451

AmazonElasticTranscoderRole	451
Utilisation de cette stratégie	451
Détails des politiques	451
Version de la politique	452
Document de stratégie JSON	452
En savoir plus	453
AmazonEMRCleanupPolicy	453
Utilisation de cette politique	453
Les des des des des	453
Version de la politique	453
Document de de de de de de	453
En savoir plus	454
AmazonEMRContainersServiceRolePolicy	454
Utilisation de cette politique politique de politique	454
détails des politiques de politique	455
Version de la politique	455
Document de stratégie JSON	455
En savoir plus	456
AmazonEMRFullAccessPolicy_v2	456
Utilisation de cette politique	456
Détails de la politique	457
Version de la politique	457
Document de politique JSON	457
En savoir plus	460
AmazonEMRReadOnlyAccessPolicy_v2	461
Utilisation de cette politique	461
Détails de la politique	461
Version de la politique	461
Document de politique JSON	461
En savoir plus	462
AmazonEMRServerlessServiceRolePolicy	462
Utilisation de cette politique	463
Détails de la politique	463
Version de la politique	463
Document de politique JSON	463
En savoir plus	464

AmazonEMRServicePolicy_v2	464
Utilisation de cette stratégie	464
Détails des politiques	465
Version de la politique	465
Document de stratégie JSON	465
En savoir plus	472
AmazonESCognitoAccess	473
Utilisation de cette stratégie	473
Détails des politiques	473
Version de la politique	473
Document de stratégie JSON	473
En savoir plus	474
AmazonESFullAccess	474
Utilisation de cette stratégie	475
Détails des politiques	475
Version de la politique	475
Document de stratégie JSON	475
En savoir plus	475
AmazonESReadOnlyAccess	476
Utilisation de cette stratégie	476
Détails des politiques	476
Version de la politique	476
Document de stratégie JSON	476
En savoir plus	477
AmazonEventBridgeApiDestinationsServiceRolePolicy	477
Utilisation de cette politique politique 	477
détails détails détails détails détails	477
Version de la politique	477
Document de stratégie JSON JSON	478
En savoir plus	478
AmazonEventBridgeFullAccess	478
Utilisation de cette stratégie	478
Détails des politiques	478
Version de la politique	479
Document de stratégie JSON	479
En savoir plus	481

AmazonEventBridgePipesFullAccess	481
Utilisation de cette stratégie	481
Détails des politiques	481
Version de la politique	482
Document de stratégie JSON	482
En savoir plus	482
AmazonEventBridgePipesOperatorAccess	483
Utilisation de cette stratégie	483
Détails des politiques	483
Version de la politique	483
Document de stratégie JSON	483
En savoir plus	484
AmazonEventBridgePipesReadOnlyAccess	484
Utilisation de cette stratégie	484
Détails des politiques	484
Version de la politique	484
Document de stratégie JSON	485
En savoir plus	485
AmazonEventBridgeReadOnlyAccess	485
Utilisation de cette stratégie	485
Détails des politiques	485
Version de la politique	486
Document de stratégie JSON	486
En savoir plus	487
AmazonEventBridgeSchedulerFullAccess	487
Utilisation de cette stratégie	488
Détails des politiques	488
Version de la politique	488
Document de stratégie JSON	488
En savoir plus	489
AmazonEventBridgeSchedulerReadOnlyAccess	489
Utilisation de cette stratégie	489
Détails des politiques	489
Version de la politique	489
Document de stratégie JSON	490
En savoir plus	490

AmazonEventBridgeSchemasFullAccess	490
Utilisation de cette stratégie	490
Détails des politiques	490
Version de la politique	491
Document de stratégie JSON	491
En savoir plus	492
AmazonEventBridgeSchemasReadOnlyAccess	492
Utilisation de cette stratégie	492
Détails des politiques	492
Version de la politique	492
Document de stratégie JSON	493
En savoir plus	493
AmazonEventBridgeSchemasServiceRolePolicy	494
En des Ides de cette politique	494
Obtenir les détails des détails	494
Version de la politique	494
Document de stratégie JSON	494
En savoir plus	495
AmazonFISServiceRolePolicy	495
Utilisation de cette politique	495
Les détails des politiques	495
Version de la politique	495
Document de stratégie JSON	496
En savoir plus	497
AmazonForecastFullAccess	497
Utilisation de cette stratégie	498
Détails des politiques	498
Version de la politique	498
Document de stratégie JSON	498
En savoir plus	499
AmazonFraudDetectorFullAccessPolicy	499
Utilisation de cette stratégie	499
Détails des politiques	499
Version de la politique	499
Document de stratégie JSON	500
En savoir plus	501

AmazonFreeRTOSFullAccess	501
Utilisation de cette stratégie	501
Détails des politiques	501
Version de la politique	501
Document de stratégie JSON	502
En savoir plus	502
AmazonFreeRTOSOTAUpdate	502
Utilisation de cette stratégie	502
Détails des stratégies	502
Version de la politique	503
Document de stratégie JSON	503
En savoir plus	504
AmazonFSxConsoleFullAccess	504
Utilisation de cette politique	504
Détails de la politique	505
Version de la politique	505
Document de politique JSON	505
En savoir plus	508
AmazonFSxConsoleReadOnlyAccess	509
Utilisation de cette politique	509
Détails de la politique	509
Version de la politique	509
Document de politique JSON	509
En savoir plus	510
AmazonFSxFullAccess	510
Utilisation de cette politique	510
Détails de la politique	510
Version de la politique	511
Document de politique JSON	511
En savoir plus	515
AmazonFSxReadOnlyAccess	515
Utilisation de cette stratégie	515
Détails des politiques	515
Version de la politique	515
Document de stratégie JSON	516
En savoir plus	516

AmazonFSxServiceRolePolicy	516
Utilisation de cette politique	516
Détails de la politique	517
Version de la politique	517
Document de politique JSON	517
En savoir plus	520
AmazonGlacierFullAccess	520
Utilisation de cette stratégie	520
Détails des politiques	520
Version de la politique	520
Document de stratégie JSON	520
En savoir plus	521
AmazonGlacierReadOnlyAccess	521
Utilisation de cette stratégie	521
Détails des politiques	521
Version de la politique	521
Document de stratégie JSON	522
En savoir plus	522
AmazonGrafanaAthenaAccess	523
Utilisation de cette stratégie	523
Détails des politiques	523
Version de la politique	523
Document de stratégie JSON	523
En savoir plus	525
AmazonGrafanaCloudWatchAccess	525
Utilisation de cette stratégie	525
Détails des politiques	525
Version de la politique	526
Document de stratégie JSON	526
En savoir plus	527
AmazonGrafanaRedshiftAccess	527
Utilisation de cette stratégie	527
Détails des politiques	527
Version de la politique	528
Document de stratégie JSON	528
En savoir plus	529

AmazonGrafanaServiceLinkedRolePolicy	529
Utilisation de cette politique	529
Les détails des politiques	530
Version de la politique	530
Document de stratégie JSON	530
En savoir plus	531
AmazonGuardDutyFullAccess	531
Utilisation de cette politique	532
Détails de la politique	532
Version de la politique	532
Document de politique JSON	532
En savoir plus	533
AmazonGuardDutyMalwareProtectionServiceRolePolicy	533
Utilisation de cette politique	534
Détails de la politique	534
Version de la politique	534
Document de politique JSON	534
En savoir plus	539
AmazonGuardDutyReadOnlyAccess	539
Utilisation de cette politique	539
Détails de la politique	539
Version de la politique	539
Document de politique JSON	540
En savoir plus	540
AmazonGuardDutyServiceRolePolicy	540
Utilisation de cette politique	541
Détails de la politique	541
Version de la politique	541
Document de politique JSON	541
En savoir plus	546
AmazonHealthLakeFullAccess	546
Utilisation de cette stratégie	546
Détails des politiques	546
Version de la politique	546
Document de stratégie JSON	547
En savoir plus	547

AmazonHealthLakeReadOnlyAccess	547
Utilisation de cette stratégie	548
Détails des politiques	548
Version de la politique	548
Document de stratégie JSON	548
En savoir plus	549
AmazonHoneycodeFullAccess	549
Utilisation de cette stratégie	549
Détails des politiques	549
Version de la politique	549
Document de stratégie JSON	549
En savoir plus	550
AmazonHoneycodeReadOnlyAccess	550
Utilisation de cette stratégie	550
Détails des politiques	550
Version de la politique	550
Document de stratégie JSON	551
En savoir plus	551
AmazonHoneycodeServiceRolePolicy	551
Utilisation de cette politique politique politique politique	551
détails des politiques politiques politiques	552
Version de la politique	552
Document de stratégie JSON document de	552
En savoir plus	552
AmazonHoneycodeTeamAssociationFullAccess	553
Utilisation de cette stratégie	553
Détails des politiques	553
Version de la politique	553
Document de stratégie JSON	553
En savoir plus	554
AmazonHoneycodeTeamAssociationReadOnlyAccess	554
Utilisation de cette stratégie	554
Détails des politiques	554
Version de la politique	554
Document de stratégie JSON	555
En savoir plus	555

AmazonHoneycodeWorkbookFullAccess	555
Utilisation de cette stratégie	555
Détails des politiques	555
Version de la politique	556
Document de stratégie JSON	556
En savoir plus	556
AmazonHoneycodeWorkbookReadOnlyAccess	557
Utilisation de cette stratégie	557
Détails des politiques	557
Version de la politique	557
Document de stratégie JSON	557
En savoir plus	558
AmazonInspector2AgentlessServiceRolePolicy	558
Utilisation de cette politique	558
Détails de la politique	558
Version de la politique	558
Document de politique JSON	559
En savoir plus	562
AmazonInspector2FullAccess	562
Utilisation de cette politique	562
Détails de la politique	563
Version de la politique	563
Document de politique JSON	563
En savoir plus	564
AmazonInspector2ManagedCisPolicy	564
Utilisation de cette politique	564
Détails de la politique	564
Version de la politique	565
Document de politique JSON	565
En savoir plus	565
AmazonInspector2ReadOnlyAccess	566
Utilisation de cette politique	566
Détails de la politique	566
Version de la politique	566
Document de politique JSON	566
En savoir plus	567

AmazonInspector2ServiceRolePolicy	567
Utilisation de cette politique	567
Détails de la politique	567
Version de la politique	568
Document de politique JSON	568
En savoir plus	574
AmazonInspectorFullAccess	574
Utilisation de cette stratégie	574
Détails des politiques	574
Version de la politique	575
Document de stratégie JSON	575
En savoir plus	576
AmazonInspectorReadOnlyAccess	576
Utilisation de cette stratégie	576
Détails des politiques	576
Version de la politique	577
Document de stratégie JSON	577
En savoir plus	577
AmazonInspectorServiceRolePolicy	578
Using this policy	578
les politiques	578
Version de la politique	578
JSON policy document	578
En savoir plus	580
AmazonKendraFullAccess	580
Utilisation de cette stratégie	580
Détails des politiques	580
Version de la politique	580
Document de stratégie JSON	580
En savoir plus	582
AmazonKendraReadOnlyAccess	582
Utilisation de cette stratégie	583
Détails des politiques	583
Version de la politique	583
Document de stratégie JSON	583
En savoir plus	584

AmazonKeyspacesFullAccess	584
Utilisation de cette politique	584
Détails de la politique	584
Version de la politique	584
Document de politique JSON	584
En savoir plus	586
AmazonKeyspacesReadOnlyAccess	586
Utilisation de cette stratégie	587
Détails des politiques	587
Version de la politique	587
Document de stratégie JSON	587
En savoir plus	588
AmazonKeyspacesReadOnlyAccess_v2	588
Utilisation de cette politique	588
Détails de la politique	588
Version de la politique	588
Document de politique JSON	589
En savoir plus	590
AmazonKinesisAnalyticsFullAccess	590
Utilisation de cette stratégie	590
Détails des politiques	590
Version de la politique	590
Document de stratégie JSON	590
En savoir plus	592
AmazonKinesisAnalyticsReadOnly	592
Utilisation de cette stratégie	592
Détails des politiques	592
Version de la politique	592
Document de stratégie JSON	593
En savoir plus	594
AmazonKinesisFirehoseFullAccess	594
Utilisation de cette stratégie	594
Détails des politiques	594
Version de la politique	595
Document de stratégie JSON	595
En savoir plus	595

AmazonKinesisFirehoseReadOnlyAccess	595
Utilisation de cette stratégie	595
Détails des politiques	596
Version de la politique	596
Document de stratégie JSON	596
En savoir plus	596
AmazonKinesisFullAccess	597
Utilisation de cette stratégie	597
Détails des politiques	597
Version de la politique	597
Document de stratégie JSON	597
En savoir plus	598
AmazonKinesisReadOnlyAccess	598
Utilisation de cette stratégie	598
Détails des politiques	598
Version de la politique	598
Document de stratégie JSON	598
En savoir plus	599
AmazonKinesisVideoStreamsFullAccess	599
Utilisation de cette stratégie	599
Détails des politiques	599
Version de la politique	600
Document de stratégie JSON	600
En savoir plus	600
AmazonKinesisVideoStreamsReadOnlyAccess	600
Utilisation de cette stratégie	600
Détails des politiques	601
Version de la politique	601
Document de stratégie JSON	601
En savoir plus	601
AmazonLaunchWizard_Fullaccess	602
Utilisation de cette stratégie	602
Détails des politiques	602
Version de la politique	602
Document de stratégie JSON	602
En savoir plus	616

AmazonLaunchWizardFullAccessV2	617
Utilisation de cette politique	617
Détails de la politique	617
Version de la politique	617
Document de politique JSON	617
En savoir plus	634
AmazonLexChannelsAccess	634
Utilisation des des des des des des	634
les des des des des	634
Version de la politique	634
d'un document de politique JSON	635
En savoir plus	635
AmazonLexFullAccess	635
Utilisation de cette politique	635
Détails de la politique	635
Version de la politique	636
Document de politique JSON	636
En savoir plus	641
AmazonLexReadOnly	641
Utilisation de cette stratégie	642
Détails des politiques	642
Version de la politique	642
Document de stratégie JSON	642
En savoir plus	643
AmazonLexReplicationPolicy	644
Utilisation de cette politique	644
Détails de la politique	644
Version de la politique	644
Document de politique JSON	644
En savoir plus	646
AmazonLexRunBotsOnly	647
Utilisation de cette stratégie	647
Détails des politiques	647
Version de la politique	647
Document de stratégie JSON	647
En savoir plus	648

AmazonLexV2BotPolicy	648
Utilisation de cette politique	648
Les détails des politiques	648
Version de la politique	648
Document de stratégie	649
En savoir plus	649
AmazonLookoutEquipmentFullAccess	649
Utilisation de cette stratégie	649
Détails des politiques	649
Version de la politique	650
Document de stratégie JSON	650
En savoir plus	651
AmazonLookoutEquipmentReadOnlyAccess	651
Utilisation de cette stratégie	651
Détails des politiques	651
Version de la politique	652
Document de stratégie JSON	652
En savoir plus	652
AmazonLookoutMetricsFullAccess	652
Utilisation de cette stratégie	653
Détails des politiques	653
Version de la politique	653
Document de stratégie JSON	653
En savoir plus	654
AmazonLookoutMetricsReadOnlyAccess	654
Utilisation de cette stratégie	654
Détails des politiques	654
Version de la politique	654
Document de stratégie JSON	655
En savoir plus	655
AmazonLookoutVisionConsoleFullAccess	656
Utilisation de cette stratégie	656
Détails des politiques	656
Version de la politique	656
Document de stratégie JSON	656
En savoir plus	658

AmazonLookoutVisionConsoleReadOnlyAccess	659
Utilisation de cette stratégie	659
Détails des politiques	659
Version de la politique	659
Document de stratégie JSON	659
En savoir plus	661
AmazonLookoutVisionFullAccess	661
Utilisation de cette stratégie	661
Détails des politiques	661
Version de la politique	661
Document de stratégie JSON	661
En savoir plus	662
AmazonLookoutVisionReadOnlyAccess	662
Utilisation de cette stratégie	662
Détails des politiques	662
Version de la politique	662
Document de stratégie JSON	663
En savoir plus	663
AmazonMachineLearningBatchPredictionsAccess	663
Utilisation de cette stratégie	664
Détails des politiques	664
Version de la politique	664
Document de stratégie JSON	664
En savoir plus	665
AmazonMachineLearningCreateOnlyAccess	665
Utilisation de cette stratégie	665
Détails des politiques	665
Version de la politique	665
Document de stratégie JSON	665
En savoir plus	666
AmazonMachineLearningFullAccess	666
Utilisation de cette stratégie	666
Détails des politiques	666
Version de la politique	667
Document de stratégie JSON	667
En savoir plus	667

AmazonMachineLearningManageRealTimeEndpointOnlyAccess	667
Utilisation de cette stratégie	668
Détails des politiques	668
Version de la politique	668
Document de stratégie JSON	668
En savoir plus	669
AmazonMachineLearningReadOnlyAccess	669
Utilisation de cette stratégie	669
Détails des politiques	669
Version de la politique	669
Document de stratégie JSON	669
En savoir plus	670
AmazonMachineLearningRealTimePredictionOnlyAccess	670
Utilisation de cette stratégie	670
Détails des politiques	670
Version de la politique	671
Document de stratégie JSON	671
En savoir plus	671
AmazonMachineLearningRoleforRedshiftDataSourceV3	671
Utilisation de cette stratégie	672
Détails des politiques	672
Version de la politique	672
Document de stratégie JSON	672
En savoir plus	673
AmazonMacieFullAccess	673
Utilisation de cette stratégie	673
Détails des politiques	673
Version de la politique	674
Document de stratégie JSON	674
En savoir plus	674
AmazonMacieHandshakeRole	675
Utilisation de cette stratégie	675
Détails des politiques	675
Version de la politique	675
Document de stratégie JSON	675
En savoir plus	676

AmazonMacieReadOnlyAccess	676
Utilisation de cette politique	676
Détails de la politique	676
Version de la politique	676
Document de politique JSON	677
En savoir plus	677
AmazonMacieServiceRole	677
Utilisation de cette stratégie	677
Détails des politiques	678
Version de la politique	678
Document de stratégie JSON	678
En savoir plus	678
AmazonMacieServiceRolePolicy	679
des politiques	679
détails des politiques	679
Version de la politique	679
document de politique JSON	679
En savoir plus	681
AmazonManagedBlockchainConsoleFullAccess	681
Utilisation de cette stratégie	681
Détails des politiques	681
Version de la politique	681
Document de stratégie JSON	681
En savoir plus	682
AmazonManagedBlockchainFullAccess	682
Utilisation de cette stratégie	682
Détails des politiques	682
Version de la politique	683
Document de stratégie JSON	683
En savoir plus	683
AmazonManagedBlockchainReadOnlyAccess	683
Utilisation de cette stratégie	684
Détails des stratégies	684
Version de la politique	684
Document de stratégie JSON	684
En savoir plus	685

AmazonManagedBlockchainServiceRolePolicy	685
Utilisation de cette politique	685
Détails des politiques	685
Version de la politique	685
Document de stratégie JSON	685
En savoir plus	686
AmazonMCSFullAccess	686
Utilisation de cette stratégie	686
Détails des politiques	686
Version de la politique	687
Document de stratégie JSON	687
En savoir plus	688
AmazonMCSReadOnlyAccess	688
Utilisation de cette stratégie	688
Détails des politiques	688
Version de la politique	689
Document de stratégie JSON	689
En savoir plus	689
AmazonMechanicalTurkFullAccess	690
Utilisation de cette stratégie	690
Détails des politiques	690
Version de la politique	690
Document de stratégie JSON	690
En savoir plus	691
AmazonMechanicalTurkReadOnly	691
Utilisation de cette stratégie	691
Détails des politiques	691
Version de la politique	691
Document de stratégie JSON	692
En savoir plus	692
AmazonMemoryDBFullAccess	692
Utilisation de la présente stratégie	692
Détails des politiques	693
Version de la politique	693
Document de stratégie JSON	693
En savoir plus	694

AmazonMemoryDBReadOnlyAccess	694
Utilisation de cette stratégie	694
Détails des politiques	694
Version de la politique	694
Document de stratégie JSON	694
En savoir plus	695
AmazonMobileAnalyticsFinancialReportAccess	695
Utilisation de cette stratégie	695
Détails des politiques	695
Version de la politique	696
Document de stratégie JSON	696
En savoir plus	696
AmazonMobileAnalyticsFullAccess	696
Utilisation de cette stratégie	697
Détails des politiques	697
Version de la politique	697
Document de stratégie JSON	697
En savoir plus	697
AmazonMobileAnalyticsNon-financialReportAccess	698
Utilisation de cette stratégie	698
Détails des politiques	698
Version de la politique	698
Document de stratégie JSON	698
En savoir plus	699
AmazonMobileAnalyticsWriteOnlyAccess	699
Utilisation de cette politique	699
Détails des politiques	699
Version de la politique	699
Document de politique JSON	700
En savoir plus	700
AmazonMonitronFullAccess	700
Utilisation de cette stratégie	700
Détails des politiques	700
Version de la politique	701
Document de stratégie JSON	701
En savoir plus	703

AmazonMQApiFullAccess	703
Utilisation de cette stratégie	703
Détails des politiques	703
Version de la politique	703
Document de stratégie JSON	703
En savoir plus	705
AmazonMQApiReadOnlyAccess	705
Utilisation de cette stratégie	705
Détails des politiques	705
Version de la politique	705
Document de stratégie JSON	705
En savoir plus	706
AmazonMQFullAccess	706
Utilisation de cette stratégie	706
Détails des politiques	706
Version de la politique	707
Document de stratégie JSON	707
En savoir plus	708
AmazonMQReadOnlyAccess	708
Utilisation de cette stratégie	708
Détails des politiques	708
Version de la politique	709
Document de stratégie JSON	709
En savoir plus	709
AmazonMQServiceRolePolicy	709
Utilisation cette politique politique politique politique.	710
Les détails politique politique politique	710
Version de la politique	710
Document politique JSON politique JSON	710
En savoir plus	712
AmazonMSKConnectReadOnlyAccess	712
Utilisation de cette stratégie	712
Détails des politiques	712
Version de la politique	713
Document de stratégie JSON	713
En savoir plus	714

AmazonMSKFullAccess	714
Utilisation de cette politique	714
Détails de la politique	714
Version de la politique	714
Document de politique JSON	715
En savoir plus	717
AmazonMSKReadOnlyAccess	718
Utilisation de cette stratégie	718
Détails des politiques	718
Version de la politique	718
Document de stratégie JSON	718
En savoir plus	719
AmazonMWAAServiceRolePolicy	719
Utilisation de cette politique	719
Les détails des politiques	719
Version de la politique	719
Document de stratégie JSON	720
En savoir plus	722
AmazonNimbleStudio-LaunchProfileWorker	722
Utilisation de cette stratégie	722
Détails des politiques	722
Version de la politique	722
Document de stratégie JSON	723
En savoir plus	723
AmazonNimbleStudio-StudioAdmin	724
Utilisation de cette politique	724
Détails de la politique	724
Version de la politique	724
Document de politique JSON	724
En savoir plus	726
AmazonNimbleStudio-StudioUser	726
Utilisation de cette politique	727
Détails de la politique	727
Version de la politique	727
Document de politique JSON	727
En savoir plus	729

AmazonOmicsFullAccess	729
Utilisation de cette stratégie	729
Détails des politiques	730
Version de la politique	730
Document de stratégie JSON	730
En savoir plus	731
AmazonOmicsReadOnlyAccess	731
Utilisation de cette stratégie	731
Détails des politiques	731
Version de la politique	732
Document de stratégie JSON	732
En savoir plus	732
AmazonOneEnterpriseFullAccess	732
Utilisation de cette politique	733
Détails de la politique	733
Version de la politique	733
Document de politique JSON	733
En savoir plus	733
AmazonOneEnterpriseInstallerAccess	734
Utilisation de cette politique	734
Détails de la politique	734
Version de la politique	734
Document de politique JSON	734
En savoir plus	735
AmazonOneEnterpriseReadOnlyAccess	735
Utilisation de cette politique	735
Détails de la politique	735
Version de la politique	736
Document de politique JSON	736
En savoir plus	736
AmazonOpenSearchDashboardsServiceRolePolicy	736
Utilisation de cette politique	737
Détails de la politique	737
Version de la politique	737
Document de politique JSON	737
En savoir plus	738

AmazonOpenSearchIngestionFullAccess	738
Utilisation de cette stratégie	738
Détails des politiques	738
Version de la politique	738
Document de stratégie JSON	738
En savoir plus	739
AmazonOpenSearchIngestionReadOnlyAccess	740
Utilisation de cette stratégie	740
Détails des politiques	740
Version de la politique	740
Document de stratégie JSON	740
En savoir plus	741
AmazonOpenSearchIngestionServiceRolePolicy	741
Utilisation de cette politique	741
des des des des des	741
Version de la politique	741
de politique J	742
En savoir plus	743
AmazonOpenSearchServerlessServiceRolePolicy	744
Utilisation de cette politique de politique	744
Détails des politiques des politiques	744
Version de la politique	744
Document de stratégie JSON	744
En savoir plus	745
AmazonOpenSearchServiceCognitoAccess	745
Utilisation de cette stratégie	745
Détails des politiques	745
Version de la politique	745
Document de stratégie JSON	746
En savoir plus	747
AmazonOpenSearchServiceFullAccess	747
Utilisation de cette stratégie	747
Détails des politiques	747
Version de la politique	747
Document de stratégie JSON	748
En savoir plus	748

AmazonOpenSearchServiceReadOnlyAccess	748
Utilisation de cette stratégie	748
Détails des politiques	748
Version de la politique	749
Document de stratégie JSON	749
En savoir plus	749
AmazonOpenSearchServiceRolePolicy	749
Utilisation de cette politique	750
Détails de la politique	750
Version de la politique	750
Document de politique JSON	750
En savoir plus	755
AmazonPersonalizeFullAccess	755
Utilisation de cette stratégie	755
Détails des politiques	755
Version de la politique	755
Document de stratégie JSON	755
En savoir plus	757
AmazonPollyFullAccess	757
Utilisation de cette stratégie	757
Détails des politiques	757
Version de la politique	757
Document de stratégie JSON	757
En savoir plus	758
AmazonPollyReadOnlyAccess	758
Utilisation de cette stratégie	758
Détails des politiques	758
Version de la politique	758
Document de stratégie JSON	759
En savoir plus	759
AmazonPrometheusConsoleFullAccess	759
Utilisation de cette stratégie	760
Détails des politiques	760
Version de la politique	760
Document de stratégie JSON	760
En savoir plus	761

AmazonPrometheusFullAccess	761
Utilisation de cette politique	761
Détails de la politique	762
Version de la politique	762
Document de politique JSON	762
En savoir plus	763
AmazonPrometheusQueryAccess	763
Utilisation de cette stratégie	763
Détails des politiques	763
Version de la politique	764
Document de stratégie JSON	764
En savoir plus	764
AmazonPrometheusRemoteWriteAccess	765
Utilisation de cette stratégie	765
Détails des politiques	765
Version de la politique	765
Document de stratégie JSON	765
En savoir plus	766
AmazonPrometheusScrapingServiceRolePolicy	766
Utilisation de cette politique	766
Détails de la politique	766
Version de la politique	766
Document de politique JSON	767
En savoir plus	769
AmazonQFullAccess	769
Utilisation de cette politique	769
Détails de la politique	769
Version de la politique	769
Document de politique JSON	769
En savoir plus	770
AmazonQLDBConsoleFullAccess	770
Utilisation de cette stratégie	770
Détails des politiques	770
Version de la politique	770
Document de stratégie JSON	771
En savoir plus	772

AmazonQLDBFullAccess	773
Utilisation de cette stratégie	773
Détails des politiques	773
Version de la politique	773
Document de stratégie JSON	773
En savoir plus	774
AmazonQLDBReadOnly	775
Utilisation de cette stratégie	775
Détails des politiques	775
Version de la politique	775
Document de stratégie JSON	775
En savoir plus	776
AmazonRDSBetaServiceRolePolicy	776
Utilisation de cette politique politique de politique	776
détails des politiques politiques politiques	776
Version de la politique	777
Document de stratégie JSON stratégie I	777
En savoir plus	780
AmazonRDSCustomInstanceProfileRolePolicy	780
Utilisation de cette politique	780
Détails de la politique	780
Version de la politique	781
Document de politique JSON	781
En savoir plus	788
AmazonRDSCustomPreviewServiceRolePolicy	788
Utilisation de cette politique	788
Détails de la politique	788
Version de la politique	789
Document de politique JSON	789
En savoir plus	804
AmazonRDSCustomServiceRolePolicy	804
Utilisation de cette politique	805
Détails de la politique	805
Version de la politique	805
Document de politique JSON	805
En savoir plus	822

AmazonRDSDDataFullAccess	822
Utilisation de cette stratégie	822
Détails des politiques	822
Version de la politique	823
Document de stratégie JSON	823
En savoir plus	824
AmazonRDSDirectoryServiceAccess	824
Utilisation de cette stratégie	824
Détails des politiques	824
Version de la politique	825
Document de stratégie JSON	825
En savoir plus	825
AmazonRDSEnhancedMonitoringRole	825
Utilisation de cette stratégie	826
Détails des politiques	826
Version de la politique	826
Document de stratégie JSON	826
En savoir plus	827
AmazonRDSFullAccess	827
Utilisation de cette politique	827
Détails de la politique	827
Version de la politique	827
Document de politique JSON	828
En savoir plus	830
AmazonRDSPerformanceInsightsFullAccess	830
Utilisation de cette politique	830
Détails de la politique	830
Version de la politique	830
Document de politique JSON	831
En savoir plus	832
AmazonRDSPerformanceInsightsReadOnly	832
Utilisation de cette politique	832
Détails de la politique	832
Version de la politique	833
Document de politique JSON	833
En savoir plus	835

AmazonRDSPreviewServiceRolePolicy	835
Utilisation de cette politique	835
Détails de la politique	835
Version de la politique	835
Document de politique JSON	835
En savoir plus	839
AmazonRDSReadOnlyAccess	839
Utilisation de cette stratégie	839
Détails des politiques	839
Version de la politique	839
Document de stratégie JSON	839
En savoir plus	841
AmazonRDSServiceRolePolicy	841
Utilisation de cette politique	841
Détails de la politique	841
Version de la politique	841
Document de politique JSON	841
En savoir plus	845
AmazonRedshiftAllCommandsFullAccess	846
Utilisation de cette politique de politique utilisée	846
Les politiques détaillées des politiques	846
Version de la politique	846
Document de stratégie JSON de politique	846
En savoir plus	851
AmazonRedshiftDataFullAccess	852
Utilisation de cette politique	852
Détails des politiques	852
Version de la politique	852
Document de stratégie JSON	852
En savoir plus	854
AmazonRedshiftFullAccess	855
Utilisation de cette stratégie	855
Détails des politiques	855
Version de la politique	855
Document de stratégie JSON	855
En savoir plus	857

AmazonRedshiftQueryEditor	857
Utilisation de cette stratégie	858
Détails des politiques	858
Version de la politique	858
Document de stratégie JSON	858
En savoir plus	860
AmazonRedshiftQueryEditorV2FullAccess	860
Utilisation de cette politique	860
Détails de la politique	860
Version de la politique	861
Document de politique JSON	861
En savoir plus	862
AmazonRedshiftQueryEditorV2NoSharing	862
Utilisation de cette politique	863
Détails de la politique	863
Version de la politique	863
Document de politique JSON	863
En savoir plus	867
AmazonRedshiftQueryEditorV2ReadSharing	867
Utilisation de cette politique	867
Détails de la politique	867
Version de la politique	868
Document de politique JSON	868
En savoir plus	873
AmazonRedshiftQueryEditorV2ReadWriteSharing	873
Utilisation de cette politique	873
Détails de la politique	873
Version de la politique	873
Document de politique JSON	874
En savoir plus	879
AmazonRedshiftReadOnlyAccess	879
Utilisation de cette politique	879
Détails de la politique	879
Version de la politique	879
Document de politique JSON	879
En savoir plus	880

AmazonRedshiftServiceLinkedRolePolicy	880
Utilisation de cette politique	880
Détails de la politique	881
Version de la politique	881
Document de politique JSON	881
En savoir plus	886
AmazonRekognitionCustomLabelsFullAccess	887
Utilisation de cette stratégie	887
Détails des politiques	887
Version de la politique	887
Document de stratégie JSON	887
En savoir plus	888
AmazonRekognitionFullAccess	889
Utilisation de cette stratégie	889
Détails des politiques	889
Version de la politique	889
Document de stratégie JSON	889
En savoir plus	890
AmazonRekognitionReadOnlyAccess	890
Utilisation de cette politique	890
Détails de la politique	890
Version de la politique	890
Document de politique JSON	891
En savoir plus	892
AmazonRekognitionServiceRole	892
Utilisation de cette stratégie	892
Détails des politiques	892
Version de la politique	892
Document de stratégie JSON	893
En savoir plus	893
AmazonRoute53AutoNamingFullAccess	894
Utilisation de cette stratégie	894
Détails des politiques	894
Version de la politique	894
Document de stratégie JSON	894
En savoir plus	895

AmazonRoute53AutoNamingReadOnlyAccess	895
Utilisation de cette stratégie	895
détails des politiques	895
Version de la politique	896
Document de stratégie JSON	896
En savoir plus	896
AmazonRoute53AutoNamingRegistrantAccess	896
Utilisation de cette stratégie	897
Détails des politiques	897
Version de la politique	897
Document de stratégie JSON	897
En savoir plus	898
AmazonRoute53DomainsFullAccess	898
Utilisation de cette stratégie	898
Détails des politiques	898
Version de la politique	898
Document de stratégie JSON	899
En savoir plus	899
AmazonRoute53DomainsReadOnlyAccess	899
Utilisation de cette stratégie	899
Détails des politiques	900
Version de la politique	900
Document de stratégie JSON	900
En savoir plus	900
AmazonRoute53FullAccess	901
Utilisation de cette stratégie	901
Détails des politiques	901
Version de la politique	901
Document de stratégie JSON	901
En savoir plus	902
AmazonRoute53ReadOnlyAccess	902
Utilisation de cette stratégie	902
Détails des politiques	903
Version de la politique	903
Document de stratégie JSON	903
En savoir plus	903

AmazonRoute53RecoveryClusterFullAccess	904
Utilisation de cette stratégie	904
Détails des politiques	904
Version de la politique	904
Document de stratégie JSON	904
En savoir plus	905
AmazonRoute53RecoveryClusterReadOnlyAccess	905
Utilisation de cette stratégie	905
Détails des politiques	905
Version de la politique	905
Document de stratégie JSON	906
En savoir plus	906
AmazonRoute53RecoveryControlConfigFullAccess	906
Utilisation de cette stratégie	906
Détails des politiques	906
Version de la politique	907
Document de stratégie JSON	907
En savoir plus	907
AmazonRoute53RecoveryControlConfigReadOnlyAccess	907
Utilisation de cette politique	908
Détails de la politique	908
Version de la politique	908
Document de politique JSON	908
En savoir plus	909
AmazonRoute53RecoveryReadinessFullAccess	909
Utilisation de cette stratégie	909
Détails des politiques	909
Version de la politique	909
Document de stratégie JSON	910
En savoir plus	910
AmazonRoute53RecoveryReadinessReadOnlyAccess	910
Utilisation de cette stratégie	910
Détails des politiques	910
Version de la politique	911
Document de stratégie JSON	911
En savoir plus	912

AmazonRoute53ResolverFullAccess	912
Utilisation de cette stratégie	912
Détails des politiques	912
Version de la politique	912
Document de stratégie JSON	913
En savoir plus	913
AmazonRoute53ResolverReadOnlyAccess	914
Utilisation de cette stratégie	914
Détails des politiques	914
Version de la politique	914
Document de stratégie JSON	914
En savoir plus	915
AmazonS3FullAccess	915
Utilisation de cette stratégie	915
Détails des politiques	915
Version de la politique	915
Document de stratégie JSON	916
En savoir plus	916
AmazonS3ObjectLambdaExecutionRolePolicy	916
Utilisation de cette stratégie	916
Détails des politiques	916
Version de la politique	917
Document de stratégie JSON	917
En savoir plus	917
AmazonS3OutpostsFullAccess	918
Utilisation de cette stratégie	918
Détails des politiques	918
Version de la politique	918
Document de stratégie JSON	918
En savoir plus	919
AmazonS3OutpostsReadOnlyAccess	919
Utilisation de cette stratégie	920
Détails des politiques	920
Version de la politique	920
Document de stratégie JSON	920
En savoir plus	921

AmazonS3ReadOnlyAccess	921
Utilisation de cette politique	921
Détails de la politique	922
Version de la politique	922
Document de politique JSON	922
En savoir plus	922
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	923
Utilisation de cette stratégie	923
Détails des politiques	923
Version de la politique	923
Document de stratégie JSON	923
En savoir plus	933
AmazonSageMakerCanvasAIServicesAccess	934
Utilisation de cette politique	934
Détails de la politique	934
Version de la politique	934
Document de politique JSON	934
En savoir plus	937
AmazonSageMakerCanvasBedrockAccess	938
Utilisation de cette politique	938
Détails de la politique	938
Version de la politique	938
Document de politique JSON	938
En savoir plus	939
AmazonSageMakerCanvasDataPrepFullAccess	939
Utilisation de cette politique	939
Détails de la politique	940
Version de la politique	940
Document de politique JSON	940
En savoir plus	947
AmazonSageMakerCanvasDirectDeployAccess	947
Utilisation de cette politique	947
Détails de la politique	947
Version de la politique	948
Document de politique JSON	948
En savoir plus	949

AmazonSageMakerCanvasForecastAccess	949
Utilisation de cette politique	949
Détails des politiques	949
Version de la politique	949
Document de stratégie JSON	950
En savoir plus	950
AmazonSageMakerCanvasFullAccess	950
Utilisation de cette politique	951
Détails de la politique	951
Version de la politique	951
Document de politique JSON	951
En savoir plus	959
AmazonSageMakerClusterInstanceRolePolicy	959
Utilisation de cette politique	959
Détails de la politique	960
Version de la politique	960
Document de politique JSON	960
En savoir plus	962
AmazonSageMakerCoreServiceRolePolicy	962
Utilisation de cette politique	962
Les détails des politiques	962
Version de la politique	962
Document de stratégie JSON	963
En savoir plus	964
AmazonSageMakerEdgeDeviceFleetPolicy	964
Utilisation de cette stratégie	964
Détails des politiques	964
Version de la politique	964
Document de stratégie JSON	964
En savoir plus	966
AmazonSageMakerFeatureStoreAccess	966
Utilisation de cette stratégie	967
Détails des politiques	967
Version de la politique	967
Document de stratégie JSON	967
En savoir plus	968

AmazonSageMakerFullAccess	968
Utilisation de cette politique	968
Détails de la politique	969
Version de la politique	969
Document de politique JSON	969
En savoir plus	985
AmazonSageMakerGeospatialExecutionRole	985
Utilisation de cette stratégie	985
Détails des politiques	985
Version de la politique	985
Document de stratégie JSON	985
En savoir plus	986
AmazonSageMakerGeospatialFullAccess	986
Utilisation de cette politique	987
Détails des politiques	987
Version de la politique	987
Document de stratégie JSON	987
En savoir plus	988
AmazonSageMakerGroundTruthExecution	988
Utilisation de cette stratégie	988
Détails des politiques	988
Version de la politique	988
Document de stratégie JSON	989
En savoir plus	992
AmazonSageMakerMechanicalTurkAccess	992
Utilisation de cette stratégie	992
Détails des politiques	993
Version de la politique	993
Document de stratégie JSON	993
En savoir plus	993
AmazonSageMakerModelGovernanceUseAccess	994
Utilisation de cette politique	994
Détails de la politique	994
Version de la politique	994
Document de politique JSON	994
En savoir plus	996

AmazonSageMakerModelRegistryFullAccess	996
Utilisation de cette stratégie	996
Détails des politiques	997
Version de la politique	997
Document de stratégie JSON	997
En savoir plus	1000
AmazonSageMakerNotebooksServiceRolePolicy	1000
Utilisation de cette politique de politique en	1000
détails détails détails détails détails	1000
Version de la politique	1001
Document de stratégie JSON	1001
En savoir plus	1004
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1004
Utilisation de cette politique	1004
Détails de la politique	1004
Version de la politique	1005
Document de politique JSON	1005
En savoir plus	1006
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1006
Utilisation de cette politique	1006
Détails de la politique	1006
Version de la politique	1006
Document de politique JSON	1007
En savoir plus	1010
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1010
Utilisation de cette politique	1011
Détails de la politique	1011
Version de la politique	1011
Document de politique JSON	1011
En savoir plus	1012
AmazonSageMakerPipelinesIntegrations	1012
Utilisation de cette politique	1012
Détails des politiques	1012
Version de la politique	1012
Document de stratégie JSON	1013
En savoir plus	1014

AmazonSageMakerReadOnly	1015
Utilisation de cette stratégie	1015
Détails des politiques	1015
Version de la politique	1015
Document de stratégie JSON	1015
En savoir plus	1016
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1017
Utilisation de cette stratégie	1017
Détails des politiques	1017
Version de la politique	1017
Document de stratégie JSON	1017
En savoir plus	1018
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1018
Utilisation de cette stratégie	1019
Détails des politiques	1019
Version de la politique	1019
Document de stratégie JSON	1019
En savoir plus	1026
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1026
Utilisation de cette stratégie	1026
Détails des politiques	1026
Version de la politique	1027
Document de stratégie JSON	1027
En savoir plus	1036
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1036
Utilisation de cette stratégie	1037
Détails des politiques	1037
Version de la politique	1037
Document de stratégie JSON	1037
En savoir plus	1039
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1039
Utilisation de cette stratégie	1039
Détails des politiques	1039
Version de la politique	1040
Document de stratégie JSON	1040
En savoir plus	1040

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1040
Utilisation de cette stratégie	1040
Détails des politiques	1041
Version de la politique	1041
Document de stratégie JSON	1041
En savoir plus	1041
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1042
Utilisation de cette stratégie	1042
Détails des politiques	1042
Version de la politique	1042
Document de stratégie JSON	1042
En savoir plus	1044
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1045
Utilisation de cette stratégie	1045
Détails des politiques	1045
Version de la politique	1045
Document de stratégie JSON	1045
En savoir plus	1055
AmazonSecurityLakeAdministrator	1055
Utilisation de cette politique	1055
Détails de la politique	1055
Version de la politique	1056
Document de politique JSON	1056
En savoir plus	1067
AmazonSecurityLakeMetastoreManager	1067
Utilisation de cette politique	1067
Détails de la politique	1067
Version de la politique	1068
Document de politique JSON	1068
En savoir plus	1070
AmazonSecurityLakePermissionsBoundary	1070
Utilisation de cette stratégie	1070
Détails des politiques	1070
Version de la politique	1070
Document de stratégie JSON	1071
En savoir plus	1074

AmazonSESEFullAccess	1074
Utilisation de cette stratégie	1074
Détails des politiques	1074
Version de la politique	1074
Document de stratégie JSON	1074
En savoir plus	1075
AmazonSESReadOnlyAccess	1075
Utilisation de cette stratégie	1075
Détails des politiques	1075
Version de la politique	1075
Document de stratégie JSON	1076
En savoir plus	1076
AmazonSNSFullAccess	1076
Utilisation de cette stratégie	1076
Détails des politiques	1076
Version de la politique	1077
Document de stratégie JSON	1077
En savoir plus	1077
AmazonSNSReadOnlyAccess	1077
Utilisation de cette stratégie	1078
Détails des politiques	1078
Version de la politique	1078
Document de stratégie JSON	1078
En savoir plus	1078
AmazonSNSRole	1079
Utilisation de cette stratégie	1079
Détails des politiques	1079
Version de la politique	1079
Document de stratégie JSON	1079
En savoir plus	1080
AmazonSQSFullAccess	1080
Utilisation de cette stratégie	1080
Détails des politiques	1080
Version de la politique	1080
Document de stratégie JSON	1081
En savoir plus	1081

AmazonSQSReadOnlyAccess	1081
Utilisation de cette stratégie	1081
Détails des politiques	1081
Version de la politique	1082
Document de stratégie JSON	1082
En savoir plus	1082
AmazonSSMAutomationApproverAccess	1083
Using this policy	1083
Policy details	1083
Version de la politique	1083
Document de stratégie JSON	1083
En savoir plus	1084
AmazonSSMAutomationRole	1084
Utilisation de cette stratégie	1084
Détails des politiques	1084
Version de la politique	1084
Document de stratégie JSON	1085
En savoir plus	1086
AmazonSSMDirectoryServiceAccess	1086
Utilisation de cette stratégie	1086
Détails des politiques	1086
Version de la politique	1087
Document de stratégie JSON	1087
En savoir plus	1087
AmazonSSMFullAccess	1087
Utilisation de cette stratégie	1088
Détails des politiques	1088
Version de la politique	1088
Document de stratégie JSON	1088
En savoir plus	1089
AmazonSSMMaintenanceWindowRole	1090
Utilisation de cette stratégie	1090
Détails des politiques	1090
Version de la politique	1090
Document de stratégie JSON	1090
En savoir plus	1092

AmazonSSMManagedEC2InstanceDefaultPolicy	1092
Utilisation de cette stratégie	1092
Détails des politiques	1092
Version de la politique	1092
Document de stratégie JSON	1092
En savoir plus	1094
AmazonSSMManagedInstanceCore	1094
Utilisation de cette stratégie	1094
Détails des politiques	1094
Version de la politique	1094
Document de stratégie JSON	1094
En savoir plus	1096
AmazonSSMPatchAssociation	1096
Utilisation de cette stratégie	1096
Détails des politiques	1096
Version de la politique	1096
Document de stratégie JSON	1097
En savoir plus	1097
AmazonSSMReadOnlyAccess	1097
Utilisation de cette stratégie	1098
Détails des politiques	1098
Version de la politique	1098
Document de stratégie JSON	1098
En savoir plus	1098
AmazonSSMServiceRolePolicy	1099
Utilisation des politiques Utilisation de cette politique	1099
Détails des politiques des politiques	1099
Version de la politique	1099
Document de stratégie JSON document de	1099
En savoir plus	1104
AmazonSumerianFullAccess	1105
Utilisation de cette stratégie	1105
Détails des politiques	1105
Version de la politique	1105
Document de stratégie JSON	1105
En savoir plus	1106

AmazonTextractFullAccess	1106
Utilisation de cette stratégie	1106
Détails des politiques	1106
Version de la politique	1106
Document de stratégie JSON	1107
En savoir plus	1107
AmazonTextractServiceRole	1107
Utilisation de cette stratégie	1107
Détails des politiques	1107
Version de la politique	1108
Document de stratégie JSON	1108
En savoir plus	1108
AmazonTimestreamConsoleFullAccess	1108
Utilisation de cette stratégie	1109
Détails des politiques	1109
Version de la politique	1109
Document de stratégie JSON	1109
En savoir plus	1111
AmazonTimestreamFullAccess	1111
Utilisation de cette stratégie	1111
Détails des politiques	1111
Version de la politique	1111
Document de stratégie JSON	1112
En savoir plus	1113
AmazonTimestreamInfluxDBFullAccess	1113
Utilisation de cette politique	1113
Détails de la politique	1113
Version de la politique	1113
Document de politique JSON	1114
En savoir plus	1116
AmazonTimestreamInfluxDBServiceRolePolicy	1116
Utilisation de cette politique	1116
Détails de la politique	1116
Version de la politique	1116
Document de politique JSON	1117
En savoir plus	1119

AmazonTimestreamReadOnlyAccess	1119
Utilisation de cette stratégie	1119
Détails des politiques	1120
Version de la politique	1120
Document de stratégie JSON	1120
En savoir plus	1121
AmazonTranscribeFullAccess	1121
Utilisation de cette stratégie	1121
Détails des politiques	1121
Version de la politique	1121
Document de stratégie JSON	1122
En savoir plus	1122
AmazonTranscribeReadOnlyAccess	1122
Utilisation de cette stratégie	1123
Détails des politiques	1123
Version de la politique	1123
Document de stratégie JSON	1123
En savoir plus	1123
AmazonVPCCrossAccountNetworkInterfaceOperations	1124
Utilisation de cette politique	1124
Détails de la politique	1124
Version de la politique	1124
Document de politique JSON	1124
En savoir plus	1126
AmazonVPCFullAccess	1126
Utilisation de cette politique	1126
Détails de la politique	1126
Version de la politique	1126
Document de politique JSON	1127
En savoir plus	1130
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1131
Utilisation de cette politique	1131
Détails de la politique	1131
Version de la politique	1131
Document de politique JSON	1131
En savoir plus	1134

AmazonVPCReachabilityAnalyzerFullAccessPolicy	1135
Utilisation de cette politique	1135
Détails de la politique	1135
Version de la politique	1135
Document de politique JSON	1135
En savoir plus	1138
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1138
Utilisation de cette stratégie	1139
Détails des politiques	1139
Version de la politique	1139
Document de stratégie JSON	1139
En savoir plus	1140
AmazonVPCReadOnlyAccess	1140
Utilisation de cette politique	1140
Détails de la politique	1140
Version de la politique	1140
Document de politique JSON	1140
En savoir plus	1142
AmazonWorkDocsFullAccess	1142
Utilisation de cette stratégie	1142
Détails des politiques	1142
Version de la politique	1142
Document de stratégie JSON	1143
En savoir plus	1143
AmazonWorkDocsReadOnlyAccess	1143
Utilisation de cette stratégie	1143
Détails des politiques	1143
Version de la politique	1144
Document de stratégie JSON	1144
En savoir plus	1144
AmazonWorkMailEventsServiceRolePolicy	1145
Using this policy	1145
détails de politique	1145
Version de la politique	1145
document de stratégie JSON	1145
En savoir plus	1146

AmazonWorkMailFullAccess	1146
Utilisation de cette stratégie	1146
Détails des politiques	1146
Version de la politique	1146
Document de stratégie JSON	1146
En savoir plus	1148
AmazonWorkMailMessageFlowFullAccess	1149
Utilisation de cette stratégie	1149
Détails des politiques	1149
Version de la politique	1149
Document de stratégie JSON	1149
En savoir plus	1150
AmazonWorkMailMessageFlowReadOnlyAccess	1150
Utilisation de cette stratégie	1150
Détails de la stratégie	1150
Version de la politique	1150
Document de stratégie JSON	1151
En savoir plus	1151
AmazonWorkMailReadOnlyAccess	1151
Utilisation de cette stratégie	1151
Détails des politiques	1151
Version de la politique	1152
Document de stratégie JSON	1152
En savoir plus	1152
AmazonWorkSpacesAdmin	1153
Utilisation de cette politique	1153
Détails de la politique	1153
Version de la politique	1153
Document de politique JSON	1153
En savoir plus	1154
AmazonWorkSpacesApplicationManagerAdminAccess	1154
Utilisation de cette stratégie	1154
Détails des politiques	1155
Version de la politique	1155
Document de stratégie JSON	1155
En savoir plus	1155

AmazonWorkspacesPCAAccess	1156
Utilisation de cette stratégie	1156
Détails des politiques	1156
Version de la politique	1156
Document de stratégie JSON	1156
En savoir plus	1157
AmazonWorkSpacesSelfServiceAccess	1157
Utilisation de cette stratégie	1157
Détails des politiques	1157
Version de la politique	1157
Document de stratégie JSON	1158
En savoir plus	1158
AmazonWorkSpacesServiceAccess	1158
Utilisation de cette stratégie	1158
Détails des politiques	1159
Version de la politique	1159
Document de stratégie JSON	1159
En savoir plus	1159
AmazonWorkSpacesWebReadOnly	1160
Utilisation de cette stratégie	1160
Détails des politiques	1160
Version de la politique	1160
Document de stratégie JSON	1160
En savoir plus	1161
AmazonWorkSpacesWebServiceRolePolicy	1161
Utilisation de cette politique	1162
Informations des des de politique	1162
Version de la politique	1162
Document de stratégie JSON document de	1162
En savoir plus	1164
AmazonZocaloFullAccess	1165
Utilisation de cette stratégie	1165
Détails des politiques	1165
Version de la politique	1165
Document de stratégie JSON	1165
En savoir plus	1166

AmazonZocaloReadOnlyAccess	1166
Utilisation de cette stratégie	1166
Détails des politiques	1166
Version de la politique	1167
Document de stratégie JSON	1167
En savoir plus	1167
AmplifyBackendDeployFullAccess	1167
Utilisation de cette politique	1168
Détails de la politique	1168
Version de la politique	1168
Document de politique JSON	1168
En savoir plus	1171
APIGatewayServiceRolePolicy	1171
Utilisation de cette politique	1172
Les détails des politiques	1172
Version de la politique	1172
Document de politique JSON	1172
En savoir plus	1174
AppIntegrationsServiceLinkedRolePolicy	1175
Utilisation des des des des des des	1175
Détails des des des des	1175
Version de la politique	1175
Document de de de de de de	1175
En savoir plus	1177
ApplicationAutoScalingForAmazonAppStreamAccess	1177
Utilisation de cette stratégie	1177
Détails des politiques	1177
Version de la politique	1178
Document de stratégie JSON	1178
En savoir plus	1178
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1179
Utilisation de cette politique	1179
Les détails des politiques	1179
Version de la politique	1179
Document de stratégie JSON	1179
En savoir plus	1181

AppRunnerNetworkingServiceRolePolicy	1181
Utilisation de de de de cette politique	1182
Utilisation des politiques	1182
Version de la politique	1182
Document de stratégie JSON	1182
En savoir plus	1183
AppRunnerServiceRolePolicy	1184
Utilisation cette politique	1184
Les politiques	1184
Version de la politique	1184
Document de politique JSON	1184
En savoir plus	1185
AutoScalingConsoleFullAccess	1185
Utilisation de cette stratégie	1185
Détails des politiques	1186
Version de la politique	1186
Document de stratégie JSON	1186
En savoir plus	1188
AutoScalingConsoleReadOnlyAccess	1188
Utilisation de cette stratégie	1188
Détails des politiques	1188
Version de la politique	1188
Document de stratégie JSON	1189
En savoir plus	1190
AutoScalingFullAccess	1190
Utilisation de cette stratégie	1190
Détails des politiques	1190
Version de la politique	1190
Document de stratégie JSON	1190
En savoir plus	1192
AutoScalingNotificationAccessRole	1192
Utilisation de cette stratégie	1192
Détails des politiques	1192
Version de la politique	1192
Document de stratégie JSON	1193
En savoir plus	1193

AutoScalingReadOnlyAccess	1193
Utilisation de cette stratégie	1193
Détails des politiques	1194
Version de la politique	1194
Document de stratégie JSON	1194
En savoir plus	1194
AutoScalingServiceRolePolicy	1195
Utilisation de cette politique	1195
Détails de la politique	1195
Version de la politique	1195
Document de politique JSON	1195
En savoir plus	1198
AWS_ConfigRole	1198
Utilisation de cette politique	1198
Détails de la politique	1198
Version de la politique	1199
Document de politique JSON	1199
En savoir plus	1230
AWSAccountActivityAccess	1230
Utilisation de la stratégie	1230
Détails des la politique	1230
Version de la politique	1230
Document de stratégie JSON	1230
En savoir plus	1231
AWSAccountManagementFullAccess	1231
Utilisation de la stratégie	1231
Détails des la stratégie	1232
Version de la politique	1232
Document de stratégie JSON	1232
En savoir plus	1232
AWSAccountManagementReadOnlyAccess	1233
Utilisation de cette stratégie	1233
Détails des politiques	1233
Version de la politique	1233
Document de stratégie JSON	1233
En savoir plus	1234

AWSAccountUsageReportAccess	1234
Utilisation de cette stratégie	1234
Détails des politiques	1234
Version de la politique	1234
Document de stratégie JSON	1234
En savoir plus	1235
AWSAgentlessDiscoveryService	1235
Utilisation de cette stratégie	1235
Détails des politiques	1235
Version de la politique	1235
Document de stratégie JSON	1236
En savoir plus	1237
AWSAppFabricFullAccess	1238
Utilisation de cette politique	1238
Détails de la politique	1238
Version de la politique	1238
Document de politique JSON	1238
En savoir plus	1240
AWSAppFabricReadOnlyAccess	1240
Utilisation de cette politique	1240
Détails de la politique	1240
Version de la politique	1240
Document de politique JSON	1240
En savoir plus	1241
AWSAppFabricServiceRolePolicy	1241
Utilisation de cette politique	1241
Détails de la politique	1241
Version de la politique	1242
Document de politique JSON	1242
En savoir plus	1243
AWSApplicationAutoscalingAppStreamFleetPolicy	1243
Utilisation de cette politique	1243
Les détails des politiques	1243
Version de la politique	1244
Document de politique JSON	1244
En savoir plus	1244

AWSApplicationAutoscalingCassandraTablePolicy	1245
Utilisation des stratégies	1245
Les détails des politiques	1245
Version de la politique	1245
Document de stratégie JSON	1245
En savoir plus	1246
AWSApplicationAutoscalingComprehendEndpointPolicy	1246
Utilisation de cette politique	1246
détails	1246
Version de la politique	1247
Document de stratégie JSON	1247
En savoir plus	1247
AWSApplicationAutoScalingCustomResourcePolicy	1247
Utilisation politique	1248
Les détails des politiques	1248
Version de la politique	1248
Document de stratégie JSON	1248
En savoir plus	1249
AWSApplicationAutoscalingDynamoDBTablePolicy	1249
Utilisation de cette politique politique politique	1249
Les détails des politiques politiques	1249
Version de la politique	1249
Document de stratégie JSON	1250
En savoir plus	1250
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1250
Utilisation de cette politique politique politique	1250
détails politiques politiques politiques	1250
Version de la politique	1251
Document de politique JSON document de	1251
En savoir plus	1251
AWSApplicationAutoscalingECSServicePolicy	1252
Utilisation de cette politique politique politique	1252
Les détails des politiques politiques	1252
Version de la politique	1252
Document de politique JSON politique de	1252
En savoir plus	1253

AWSApplicationAutoscalingElastiCacheRGPolicy	1253
Utilisation de cette politique de politique Utilisation	1253
Utilisation des politiques politiques politiques	1253
Version de la politique	1254
Document de politique JSON des politiques	1254
En savoir plus	1255
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1255
Utilisation de cette politique	1255
Les détails des politiques	1255
Version de la politique	1255
Document de stratégie de stratégie de stratégie	1256
En savoir plus	1256
AWSApplicationAutoscalingKafkaClusterPolicy	1256
Utilisation de cette politique	1256
détails de politique	1256
Version de la politique	1257
Document de stratégie JSON	1257
En savoir plus	1257
AWSApplicationAutoscalingLambdaConcurrencyPolicy	1258
Utilisation de cette politique	1258
Détails des politiques	1258
Version de la politique	1258
Document de politique JSON	1258
En savoir plus	1259
AWSApplicationAutoscalingNeptuneClusterPolicy	1259
Using this policy	1259
Policy details	1259
Version de la politique	1259
JSON policy document	1260
En savoir plus	1261
AWSApplicationAutoscalingRDSClusterPolicy	1261
Utilisation des stratégies IAM	1261
Détails des politiques	1262
Version de la politique	1262
Document de stratégie JSON Document de	1262
En savoir plus	1263

AWSApplicationAutoscalingSageMakerEndpointPolicy	1263
Utilisation de cette politique	1263
Détails de la politique	1263
Version de la politique	1263
Document de politique JSON	1264
En savoir plus	1264
AWSApplicationDiscoveryAgentAccess	1265
Utilisation de cette stratégie	1265
Détails des politiques	1265
Version de la politique	1265
Document de stratégie JSON	1265
En savoir plus	1266
AWSApplicationDiscoveryAgentlessCollectorAccess	1266
Utilisation de cette stratégie	1266
Détails des politiques	1266
Version de la politique	1267
Document de stratégie JSON	1267
En savoir plus	1268
AWSApplicationDiscoveryServiceFullAccess	1268
Utilisation de cette stratégie	1268
Détails des politiques	1268
Version de la politique	1268
Document de stratégie JSON	1269
En savoir plus	1270
AWSApplicationMigrationAgentInstallationPolicy	1270
Utilisation de cette stratégie	1271
Détails des politiques	1271
Version de la politique	1271
Document de stratégie JSON	1271
En savoir plus	1272
AWSApplicationMigrationAgentPolicy	1272
Utilisation de cette stratégie	1272
Détails des politiques	1273
Version de la politique	1273
Document de stratégie JSON	1273
En savoir plus	1274

AWSApplicationMigrationAgentPolicy_v2	1274
Utilisation de cette stratégie	1274
Détails des stratégies	1274
Version de la politique	1275
Document de stratégie JSON SON SON	1275
En savoir plus	1275
AWSApplicationMigrationConversionServerPolicy	1276
Utilisation de cette stratégie	1276
Détails des politiques	1276
Version de la politique	1276
Document de stratégie JSON	1277
En savoir plus	1277
AWSApplicationMigrationEC2Access	1277
Utilisation de cette stratégie	1277
Détails des politiques	1277
Version de la politique	1278
Document de stratégie JSON	1278
En savoir plus	1286
AWSApplicationMigrationFullAccess	1286
Utilisation de cette stratégie	1286
Détails des politiques	1286
Version de la politique	1286
Document de stratégie JSON	1286
En savoir plus	1292
AWSApplicationMigrationMGHAccess	1292
Utilisation de cette stratégie	1292
Détails de la politique	1292
Version de la politique	1292
Document de stratégie JSON document de	1293
En savoir plus	1293
AWSApplicationMigrationReadOnlyAccess	1293
Utilisation de cette stratégie	1294
Détails des politiques	1294
Version de la politique	1294
Document de stratégie JSON	1294
En savoir plus	1295

AWSApplicationMigrationReplicationServerPolicy	1295
Utilisation de cette stratégie	1296
Détails des stratégies	1296
Version de la politique	1296
Document de stratégie JSON	1296
En savoir plus	1298
AWSApplicationMigrationServiceEc2InstancePolicy	1298
Utilisation de cette politique	1298
Détails de la politique	1298
Version de la politique	1299
Document de politique JSON	1299
En savoir plus	1300
AWSApplicationMigrationServiceRolePolicy	1300
Utilisation de cette politique	1300
Détails de la politique	1300
Version de la politique	1301
Document de politique JSON	1301
En savoir plus	1308
AWSApplicationMigrationSSMAccess	1308
Utilisation de cette stratégie	1308
Détails des politiques	1308
Version de la politique	1309
Document de stratégie JSON	1309
En savoir plus	1311
AWSApplicationMigrationVCenterClientPolicy	1311
Utilisation de cette stratégie	1311
Détails des politiques	1311
Version de la politique	1311
Document de stratégie JSON	1312
En savoir plus	1312
AWSAppMeshEnvoyAccess	1312
Utilisation de cette stratégie	1313
Détails des politiques	1313
Version de la politique	1313
Document de stratégie JSON	1313
En savoir plus	1313

AWSAppMeshFullAccess	1314
Utilisation de cette stratégie	1314
Détails des politiques	1314
Version de la politique	1314
Document de stratégie JSON	1314
En savoir plus	1316
AWSAppMeshPreviewEnvoyAccess	1316
Utilisation de cette stratégie	1316
Détails des politiques	1316
Version de la politique	1316
Document de stratégie JSON	1316
En savoir plus	1317
AWSAppMeshPreviewServiceRolePolicy	1317
Utilisation de cette politique	1317
Les détails des politiques	1317
Version de la politique	1318
Document de politique JSON	1318
En savoir plus	1318
AWSAppMeshReadOnly	1319
Utilisation de cette stratégie	1319
Détails des politiques	1319
Version de la politique	1319
Document de stratégie JSON	1319
En savoir plus	1320
AWSAppMeshServiceRolePolicy	1320
Utilisation de cette politique	1321
Détails de la politique	1321
Version de la politique	1321
Document de politique JSON	1321
En savoir plus	1322
AWSAppRunnerFullAccess	1322
Utilisation de cette stratégie	1322
Détails des politiques	1322
Version de la politique	1322
Document de stratégie JSON	1322
En savoir plus	1323

AWSAppRunnerReadOnlyAccess	1324
Utilisation de cette politique	1324
Détails des politiques	1324
Version de la politique	1324
Document de stratégie JSON	1324
En savoir plus	1325
AWSAppRunnerServicePolicyForECRAccess	1325
Utilisation de cette stratégie	1325
Détails des politiques	1325
Version de la politique	1325
Document de stratégie JSON	1326
En savoir plus	1326
AWSAppSyncAdministrator	1326
Utilisation de cette stratégie	1326
Détails des politiques	1326
Version de la politique	1327
Document de stratégie JSON	1327
En savoir plus	1328
AWSAppSyncInvokeFullAccess	1328
Utilisation de cette stratégie	1328
Détails des politiques	1328
Version de la politique	1329
Document de stratégie JSON	1329
En savoir plus	1329
AWSAppSyncPushToCloudWatchLogs	1330
Utilisation de cette stratégie	1330
Détails des politiques	1330
Version de la politique	1330
Document de stratégie JSON	1330
En savoir plus	1331
AWSAppSyncSchemaAuthor	1331
Utilisation de cette stratégie	1331
Détails des politiques	1331
Version de la politique	1331
Document de politique JSON	1332
En savoir plus	1333

AWSAppSyncServiceRolePolicy	1333
Utilisation cette politique	1333
Les détails des politiques	1333
Version de la politique	1333
Document de stratégie JSON	1333
En savoir plus	1334
AWSArtifactAccountSync	1334
Utilisation de cette stratégie	1334
Détails des politiques	1334
Version de la politique	1335
Document de stratégie JSON	1335
En savoir plus	1335
AWSArtifactReportsReadOnlyAccess	1335
Utilisation de cette politique	1336
Détails de la politique	1336
Version de la politique	1336
Document de politique JSON	1336
En savoir plus	1337
AWSArtifactServiceRolePolicy	1337
Utilisation de cette politique	1337
Détails de la politique	1337
Version de la politique	1337
Document de politique JSON	1337
En savoir plus	1338
AWSAuditManagerAdministratorAccess	1338
Utilisation de cette stratégie	1338
Détails des politiques	1338
Version de la politique	1339
Document de stratégie JSON	1339
En savoir plus	1342
AWSAuditManagerServiceRolePolicy	1343
Utilisation de cette politique	1343
Détails de la politique	1343
Version de la politique	1343
Document de politique JSON	1343
En savoir plus	1348

AWSAutoScalingPlansEC2AutoScalingPolicy	1348
Utilisation de cette politique	1348
Les détails des politiques	1348
Version de la politique	1348
Document de stratégie JSON	1349
En savoir plus	1349
AWSBackupAuditAccess	1349
Utilisation de cette stratégie	1350
Détails des politiques	1350
Version de la politique	1350
Document de stratégie JSON	1350
En savoir plus	1351
AWSBackupDataTransferAccess	1352
Utilisation de cette stratégie	1352
Détails des politiques	1352
Version de la politique	1352
Document de stratégie JSON	1352
En savoir plus	1353
AWSBackupFullAccess	1353
Utilisation de cette politique	1353
Détails de la politique	1353
Version de la politique	1353
Document de politique JSON	1354
En savoir plus	1363
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	1364
Utilisation de cette stratégie	1364
Détails des politiques	1364
Version de la politique	1364
Document de stratégie JSON	1364
En savoir plus	1365
AWSBackupOperatorAccess	1365
Utilisation de cette politique	1365
Détails de la politique	1365
Version de la politique	1366
Document de politique JSON	1366
En savoir plus	1372

AWSBackupOrganizationAdminAccess	1373
Utilisation de cette stratégie	1373
Détails des politiques	1373
Version de la politique	1373
Document de stratégie JSON	1373
En savoir plus	1375
AWSBackupRestoreAccessForSAPHANA	1375
Utilisation de cette stratégie	1376
Détails des politiques	1376
Version de la politique	1376
Document de stratégie JSON	1376
En savoir plus	1377
AWSBackupServiceLinkedRolePolicyForBackup	1377
Utilisation de cette politique	1377
Détails de la politique	1377
Version de la politique	1378
Document de politique JSON	1378
En savoir plus	1386
AWSBackupServiceLinkedRolePolicyForBackupTest	1386
Utilisation de de de de de de	1386
Les politiques politiques de politique	1386
Version de la politique	1386
Document de stratégie JSON politique J	1386
En savoir plus	1387
AWSBackupServiceRolePolicyForBackup	1387
Utilisation de cette politique	1387
Détails de la politique	1388
Version de la politique	1388
Document de politique JSON	1388
En savoir plus	1399
AWSBackupServiceRolePolicyForRestores	1399
Utilisation de cette politique	1399
Détails de la politique	1399
Version de la politique	1399
Document de politique JSON	1400
En savoir plus	1409

AWSBackupServiceRolePolicyForS3Backup	1410
Utilisation de cette stratégie	1410
Détails des politiques	1410
Version de la politique	1410
Document de stratégie JSON	1410
En savoir plus	1412
AWSBackupServiceRolePolicyForS3Restore	1412
Utilisation de cette stratégie	1413
Détails des politiques	1413
Version de la politique	1413
Document de stratégie JSON	1413
En savoir plus	1414
AWSBatchFullAccess	1415
Utilisation de cette stratégie	1415
Détails des politiques	1415
Version de la politique	1415
Document de stratégie JSON	1415
En savoir plus	1417
AWSBatchServiceEventTargetRole	1417
Utilisation de cette stratégie	1417
Détails des politiques	1417
Version de la politique	1417
Document de stratégie JSON	1418
En savoir plus	1418
AWSBatchServiceRole	1418
Utilisation de cette politique	1418
Détails de la politique	1418
Version de la politique	1419
Document de politique JSON	1419
En savoir plus	1422
AWSBillingConductorFullAccess	1422
Utilisation de cette stratégie	1422
Détails des politiques	1422
Version de la politique	1423
Document de stratégie JSON	1423
En savoir plus	1423

AWSBillingConductorReadOnlyAccess	1423
Utilisation de cette politique	1424
Détails des politiques	1424
Version de la politique	1424
Document de politique JSON	1424
En savoir plus	1425
AWSBillingReadOnlyAccess	1425
Utilisation de cette politique	1425
Détails de la politique	1425
Version de la politique	1425
Document de politique JSON	1425
En savoir plus	1427
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	1427
Utilisation de cette stratégie	1427
Détails des politiques	1427
Version de la politique	1428
Document de stratégie JSON	1428
En savoir plus	1429
AWSBudgetsActionsWithAWSResourceControlAccess	1429
Utilisation de cette stratégie	1429
Détails des politiques	1429
Version de la politique	1429
Document de stratégie JSON	1430
En savoir plus	1431
AWSBudgetsReadOnlyAccess	1431
Utilisation de cette stratégie	1431
Détails des politiques	1431
Version de la politique	1431
Document de stratégie JSON	1432
En savoir plus	1432
AWSBugBustFullAccess	1432
Utilisation de cette stratégie	1432
Détails des politiques	1433
Version de la politique	1433
Document de stratégie JSON	1433
En savoir plus	1434

AWSBugBustPlayerAccess	1434
Utilisation de cette stratégie	1434
Détails des politiques	1435
Version de la politique	1435
Document de stratégie JSON	1435
En savoir plus	1436
AWSBugBustServiceRolePolicy	1436
Utilisation	1436
Détails	1436
Version de la politique	1437
Document politique JSON	1437
En savoir plus	1437
AWSCertificateManagerFullAccess	1438
Utilisation de cette stratégie	1438
Détails des politiques	1438
Version de la politique	1438
Document de stratégie JSON	1438
En savoir plus	1439
AWSCertificateManagerPrivateCAAuditor	1439
Utilisation de cette stratégie	1439
Détails des politiques	1440
Version de la politique	1440
Document de stratégie JSON	1440
En savoir plus	1441
AWSCertificateManagerPrivateCAFullAccess	1441
Utilisation de cette stratégie	1441
Détails de la stratégie	1441
Version de la politique	1441
Document de stratégie JSON	1442
En savoir plus	1442
AWSCertificateManagerPrivateCAPrivilegedUser	1442
Utilisation de cette stratégie	1442
Détails des politiques	1442
Version de la politique	1443
Document de stratégie JSON	1443
En savoir plus	1444

AWSCertificateManagerPrivateCAReadOnly	1444
Utilisation de cette stratégie	1444
Détails de la stratégie	1444
Version de la politique	1445
Document de stratégie JSON	1445
En savoir plus	1445
AWSCertificateManagerPrivateCAUser	1446
Utilisation de cette stratégie	1446
Détails de la stratégie	1446
Version de la politique	1446
Document de stratégie JSON	1446
En savoir plus	1447
AWSCertificateManagerReadOnly	1448
Utilisation de cette stratégie	1448
Détails des politiques	1448
Version de la politique	1448
Document de stratégie JSON	1448
En savoir plus	1449
AWSChatbotServiceLinkedRolePolicy	1449
Utilisation des stratégies IAM	1449
Détails des détails des politiques	1449
Version de la politique	1449
Document de stratégie JAM	1450
En savoir plus	1450
AWSCleanRoomsFullAccess	1451
Utilisation de cette politique	1451
Détails de la politique	1451
Version de la politique	1451
Document de politique JSON	1451
En savoir plus	1456
AWSCleanRoomsFullAccessNoQuerying	1456
Utilisation de cette politique	1456
Détails de la politique	1456
Version de la politique	1456
Document de politique JSON	1456
En savoir plus	1461

AWSCleanRoomsMLFullAccess	1461
Utilisation de cette politique	1461
Détails de la politique	1462
Version de la politique	1462
Document de politique JSON	1462
En savoir plus	1466
AWSCleanRoomsMLReadOnlyAccess	1466
Utilisation de cette politique	1466
Détails de la politique	1466
Version de la politique	1466
Document de politique JSON	1466
En savoir plus	1467
AWSCleanRoomsReadOnlyAccess	1468
Utilisation de cette stratégie	1468
Détails des politiques	1468
Version de la politique	1468
Document de stratégie JSON	1468
En savoir plus	1469
AWSCloud9Administrator	1470
Utilisation de cette politique	1470
Détails de la politique	1470
Version de la politique	1470
Document de politique JSON	1470
En savoir plus	1472
AWSCloud9EnvironmentMember	1472
Utilisation de cette politique	1472
Détails de la politique	1472
Version de la politique	1472
Document de politique JSON	1472
En savoir plus	1474
AWSCloud9ServiceRolePolicy	1474
Utilisation de cette politique	1474
Les détails des politiques	1474
Version de la politique	1474
Document de stratégie JSON	1475
En savoir plus	1477

AWSCloud9SSMInstanceProfile	1477
Utilisation de cette stratégie	1477
Détails des politiques	1477
Version de la politique	1478
Document de stratégie JSON	1478
En savoir plus	1478
AWSCloud9User	1479
Utilisation de cette politique	1479
Détails de la politique	1479
Version de la politique	1479
Document de politique JSON	1479
En savoir plus	1481
AWSCloudFormationFullAccess	1482
Utilisation de cette stratégie	1482
Détails des politiques	1482
Version de la politique	1482
Document de stratégie JSON	1482
En savoir plus	1483
AWSCloudFormationReadOnlyAccess	1483
Utilisation de cette stratégie	1483
Détails des politiques	1483
Version de la politique	1483
Document de stratégie JSON	1484
En savoir plus	1484
AWSCloudFrontLogger	1484
Utilisation des de de de de cette politique	1484
Les détails des des politiques	1485
Version de la politique	1485
Document de stratégie JSON	1485
En savoir plus	1485
AWSCloudHSMFullAccess	1486
Utilisation de cette stratégie	1486
Détails des politiques	1486
Version de la politique	1486
Document de stratégie JSON	1486
En savoir plus	1487

AWSCloudHSMReadOnlyAccess	1487
Utilisation de cette stratégie	1487
Détails des politiques	1487
Version de la politique	1487
Document de stratégie JSON	1487
En savoir plus	1488
AWSCloudHSMRole	1488
Utilisation de cette stratégie	1488
Détails des politiques	1488
Version de la politique	1488
Document de stratégie JSON	1489
En savoir plus	1489
AWSCloudMapDiscoverInstanceAccess	1489
Utilisation de cette politique	1490
Détails de la politique	1490
Version de la politique	1490
Document de politique JSON	1490
En savoir plus	1491
AWSCloudMapFullAccess	1491
Utilisation de cette stratégie	1491
Détails des politiques	1491
Version de la politique	1491
Document de stratégie JSON	1491
En savoir plus	1492
AWSCloudMapReadOnlyAccess	1492
Utilisation de cette politique	1492
Détails de la politique	1493
Version de la politique	1493
Document de politique JSON	1493
En savoir plus	1493
AWSCloudMapRegisterInstanceAccess	1494
Utilisation de cette politique	1494
Détails de la politique	1494
Version de la politique	1494
Document de politique JSON	1494
En savoir plus	1495

AWSCloudShellFullAccess	1495
Utilisation de cette stratégie	1495
Détails des politiques	1495
Version de la politique	1496
Document de stratégie JSON	1496
En savoir plus	1496
AWSCloudTrail_FullAccess	1496
Utilisation de cette stratégie	1497
Détails des politiques	1497
Version de la politique	1497
Document de stratégie JSON	1497
En savoir plus	1500
AWSCloudTrail_ReadOnlyAccess	1500
Utilisation de cette stratégie	1500
Détails des politiques	1500
Version de la politique	1500
Document de politique JSON	1500
En savoir plus	1501
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	1501
Utilisation politique	1501
détails détails détails détails politiques	1501
Version de la politique	1502
Document stratégie JSON	1502
En savoir plus	1502
AWSCodeArtifactAdminAccess	1502
Utilisation de cette stratégie	1502
Détails des politiques	1503
Version de la politique	1503
Document de stratégie JSON	1503
En savoir plus	1504
AWSCodeArtifactReadOnlyAccess	1504
Utilisation de cette stratégie	1504
Détails des politiques	1504
Version de la politique	1504
Document de stratégie JSON	1504
En savoir plus	1505

AWSCodeBuildAdminAccess	1505
Utilisation de cette politique	1505
Détails de la politique	1506
Version de la politique	1506
Document de politique JSON	1506
En savoir plus	1509
AWSCodeBuildDeveloperAccess	1509
Utilisation de cette politique	1510
Détails de la politique	1510
Version de la politique	1510
Document de politique JSON	1510
En savoir plus	1513
AWSCodeBuildReadOnlyAccess	1513
Utilisation de cette stratégie	1513
Détails des politiques	1513
Version de la politique	1513
Document de stratégie JSON	1514
En savoir plus	1515
AWSCodeCommitFullAccess	1515
Utilisation de cette politique	1515
Détails de la politique	1515
Version de la politique	1516
Document de politique JSON	1516
En savoir plus	1520
AWSCodeCommitPowerUser	1521
Utilisation de cette politique	1521
Détails de la politique	1521
Version de la politique	1521
Document de politique JSON	1521
En savoir plus	1526
AWSCodeCommitReadOnly	1526
Utilisation de cette stratégie	1526
Détails des politiques	1526
Version de la politique	1527
Document de stratégie JSON	1527
En savoir plus	1529

AWSCodeDeployDeployerAccess	1530
Utilisation de cette stratégie	1530
Détails des politiques	1530
Version de la politique	1530
Document de stratégie JSON	1530
En savoir plus	1532
AWSCodeDeployFullAccess	1532
Utilisation de cette stratégie	1532
Détails des politiques	1532
Version de la politique	1532
Document de stratégie JSON	1533
En savoir plus	1534
AWSCodeDeployReadOnlyAccess	1534
Utilisation de cette stratégie	1534
Détails des politiques	1535
Version de la politique	1535
Document de stratégie JSON	1535
En savoir plus	1536
AWSCodeDeployRole	1536
Utilisation de cette politique	1536
Détails de la politique	1536
Version de la politique	1537
Document de politique JSON	1537
En savoir plus	1538
AWSCodeDeployRoleForCloudFormation	1538
Utilisation de cette stratégie	1538
Détails des politiques	1539
Version de la politique	1539
Document de stratégie JSON	1539
En savoir plus	1539
AWSCodeDeployRoleForECS	1540
Utilisation de cette stratégie	1540
Détails des politiques	1540
Version de la politique	1540
Document de stratégie JSON	1540
En savoir plus	1541

AWSCodeDeployRoleForECSLimited	1542
Utilisation de cette stratégie	1542
Détails des politiques	1542
Version de la politique	1542
Document de stratégie JSON	1542
En savoir plus	1544
AWSCodeDeployRoleForLambda	1544
Utilisation de cette stratégie	1544
Détails des politiques	1544
Version de la politique	1545
Document de stratégie JSON	1545
En savoir plus	1546
AWSCodeDeployRoleForLambdaLimited	1546
Utilisation de cette stratégie	1546
Détails des politiques	1546
Version de la politique	1547
Document de stratégie JSON	1547
En savoir plus	1548
AWSCodePipeline_FullAccess	1548
Utilisation de cette politique	1548
Détails de la politique	1548
Version de la politique	1548
Document de politique JSON	1549
En savoir plus	1552
AWSCodePipeline_ReadOnlyAccess	1553
Utilisation de cette stratégie	1553
Détails des politiques	1553
Version de la politique	1553
Document de stratégie JSON	1553
En savoir plus	1554
AWSCodePipelineApproverAccess	1555
Utilisation de cette stratégie	1555
Détails des politiques	1555
Version de la politique	1555
Document de stratégie JSON	1555
En savoir plus	1556

AWSCodePipelineCustomActionAccess	1556
Utilisation de cette stratégie	1556
Détails des politiques	1556
Version de la politique	1556
Document de stratégie JSON	1557
En savoir plus	1557
AWSCodeStarFullAccess	1557
Utilisation de cette stratégie	1557
Détails des politiques	1557
Version de la politique	1558
Document de stratégie JSON	1558
En savoir plus	1559
AWSCodeStarNotificationsServiceRolePolicy	1559
Utilisation des politique de politique de politique	1559
détails des politique de politique	1559
Version de la politique	1559
document de politique JSON politique J	1560
En savoir plus	1561
AWSCodeStarServiceRole	1561
Utilisation de cette stratégie	1561
Détails des politiques	1561
Version de la politique	1561
Document de stratégie JSON	1562
En savoir plus	1566
AWSCompromisedKeyQuarantine	1567
Utilisation de cette stratégie	1567
Détails des politiques	1567
Version de la politique	1567
Document de stratégie JSON	1567
En savoir plus	1568
AWSCompromisedKeyQuarantineV2	1569
Utilisation de cette stratégie	1569
Détails de la stratégie	1569
Version de la politique	1569
Document de stratégie JSON	1569
En savoir plus	1571

AWSCfgMultiAccountSetupPolicy	1571
Utilisation de de de de de de	1571
Détails des des des politique	1571
Version de la politique	1572
Document de politique JSON	1572
En savoir plus	1574
AWSCfgRemediationServiceRolePolicy	1574
Utilisation de cette politique de politique de	1574
Détails des politiques de politique	1574
Version de la politique	1574
Document de stratégie JSON de stratégie	1575
En savoir plus	1575
AWSCfgRoleForOrganizations	1576
Utilisation de cette stratégie	1576
Détails des politiques	1576
Version de la politique	1576
Document de stratégie JSON	1576
En savoir plus	1577
AWSCfgRulesExecutionRole	1577
Utilisation de cette stratégie	1577
Détails des politiques	1577
Version de la politique	1577
Document de stratégie JSON	1578
En savoir plus	1578
AWSCfgServiceRolePolicy	1578
Utilisation de cette politique	1579
Détails de la politique	1579
Version de la politique	1579
Document de politique JSON	1579
En savoir plus	1611
AWSCfgUserAccess	1611
Utilisation de cette politique	1611
Détails des politiques	1611
Version de la politique	1611
Document de stratégie JSON	1611
En savoir plus	1612

AWSCongressionalAccountServiceRolePolicy	1612
Utilisation de cette politique	1612
Détails de la politique	1612
Version de la politique	1613
Document de politique JSON	1613
En savoir plus	1615
AWSCongressionalAccountServiceRolePolicy	1615
Utilisation de politiques	1615
détails des politiques	1615
Version de la politique	1615
Document de politique JSON	1616
En savoir plus	1617
AWSCongressionalServiceRolePolicy	1618
Utilisation de cette stratégie	1618
Détails des politiques	1618
Version de la politique	1618
Document de stratégie JSON	1618
En savoir plus	1623
AWSCongressionalUsageReportAutomationPolicy	1623
Utilisation de cette stratégie	1623
Détails des politiques	1623
Version de la politique	1623
Document de stratégie JSON	1624
En savoir plus	1625
AWSCongressionalFullAccess	1625
Utilisation de cette politique	1625
Détails des politiques	1625
Version de la politique	1625
Document de politique JSON	1626
En savoir plus	1629
AWSCongressionalProviderFullAccess	1629
Utilisation de la politique	1629
Détails des politiques	1629
Version de la politique	1629
Document de stratégie JSON	1630
En savoir plus	1633

AWSDataExchangeReadOnly	1633
Utilisation de cette stratégie	1633
Détails des politiques	1634
Version de la politique	1634
Document de stratégie JSON	1634
En savoir plus	1635
AWSDataExchangeSubscriberFullAccess	1635
Utilisation de cette politique	1635
Détails des politiques	1635
Version de la politique	1635
Document de stratégie JSON	1636
En savoir plus	1638
AWSDataLifecycleManagerServiceRole	1638
Utilisation de cette stratégie	1638
Détails des politiques	1638
Version de la politique	1638
Document de stratégie JSON	1639
En savoir plus	1640
AWSDataLifecycleManagerServiceRoleForAMIManagement	1640
Utilisation de cette stratégie	1640
Détails des politiques	1640
Version de la politique	1640
Document de stratégie JSON	1641
En savoir plus	1642
AWSDataLifecycleManagerSSMFullAccess	1642
Utilisation de cette politique	1642
Détails de la politique	1642
Version de la politique	1643
Document de politique JSON	1643
En savoir plus	1644
AWSDataPipeline_FullAccess	1644
Utilisation de cette stratégie	1644
Détails des politiques	1645
Version de la politique	1645
Document de stratégie JSON	1645
En savoir plus	1646

AWSDatapipeline_PowerUser	1646
Utilisation de la présente stratégie	1646
Détails des politiques	1646
Version de la politique	1647
Document de stratégie JSON	1647
En savoir plus	1648
AWSDatasyncDiscoveryServiceRolePolicy	1648
Utilisation de cette politique	1648
Les détails des politiques	1648
Version de la politique	1648
Document de stratégie JSON	1649
En savoir plus	1650
AWSDatasyncFullAccess	1650
Utilisation de cette politique	1650
Détails de la politique	1650
Version de la politique	1650
Document de politique JSON	1650
En savoir plus	1652
AWSDatasyncReadOnlyAccess	1652
Utilisation de cette stratégie	1652
Détails des politiques	1652
Version de la politique	1652
Document de stratégie JSON	1652
En savoir plus	1653
AWSDeepLensLambdaFunctionAccessPolicy	1653
Utilisation de cette stratégie	1654
Détails des politiques	1654
Version de la politique	1654
Document de stratégie JSON	1654
En savoir plus	1655
AWSDeepLensServiceRolePolicy	1656
Utilisation de cette stratégie	1656
Détails des politiques	1656
Version de la politique	1656
Document de stratégie JSON	1656
En savoir plus	1663

AWSDeepRacerAccountAdminAccess	1664
Utilisation de cette stratégie	1664
Détails des politiques	1664
Version de la politique	1664
Document de stratégie JSON	1664
En savoir plus	1665
AWSDeepRacerCloudFormationAccessPolicy	1665
Utilisation de cette stratégie	1665
Détails des politiques	1665
Version de la politique	1665
Document de stratégie JSON	1666
En savoir plus	1669
AWSDeepRacerDefaultMultiUserAccess	1669
Utilisation de cette stratégie	1669
Détails des politiques	1669
Version de la politique	1669
Document de stratégie JSON	1669
En savoir plus	1671
AWSDeepRacerFullAccess	1671
Utilisation de cette stratégie	1671
Détails des politiques	1671
Version de la politique	1672
Document de stratégie JSON	1672
En savoir plus	1673
AWSDeepRacerRoboMakerAccessPolicy	1673
Utilisation de cette stratégie	1673
Détails des politiques	1673
Version de la politique	1673
Document de stratégie JSON	1674
En savoir plus	1675
AWSDeepRacerServiceRolePolicy	1676
Utilisation de cette stratégie	1676
Détails des politiques	1676
Version de la politique	1676
Document de stratégie JSON	1676
En savoir plus	1679

AWSDenyAll	1680
Utilisation de cette politique	1680
Détails de la politique	1680
Version de la politique	1680
Document de politique JSON	1680
En savoir plus	1681
AWSDeviceFarmFullAccess	1681
Utilisation de cette stratégie	1681
Détails des politiques	1681
Version de la politique	1681
Document de stratégie JSON	1681
En savoir plus	1682
AWSDeviceFarmServiceRolePolicy	1682
Utilisation de cette politique	1682
Les détails des politiques	1682
Version de la politique	1683
Document de politique JSON	1683
En savoir plus	1685
AWSDeviceFarmTestGridServiceRolePolicy	1685
Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation	1685
Les détails	1685
Version de la politique	1685
Document de stratégie JSON	1686
En savoir plus	1688
AWSDirectConnectFullAccess	1688
Utilisation de cette stratégie	1688
Détails des politiques	1688
Version de la politique	1688
Document de stratégie JSON	1689
En savoir plus	1689
AWSDirectConnectReadOnlyAccess	1689
Utilisation de cette stratégie	1689
Détails des politiques	1689
Version de la politique	1690
Document de stratégie JSON	1690
En savoir plus	1690

AWSDirectConnectServiceRolePolicy	1691
Utilisation de cette politique	1691
Les détails des politiques	1691
Version de la politique	1691
Document de stratégie JSON	1691
En savoir plus	1692
AWSDirectoryServiceFullAccess	1692
Utilisation de cette stratégie	1692
Détails des politiques	1692
Version de la politique	1692
Document de stratégie JSON	1693
En savoir plus	1694
AWSDirectoryServiceReadOnlyAccess	1695
Utilisation de cette stratégie	1695
Détails des politiques	1695
Version de la politique	1695
Document de stratégie JSON	1695
En savoir plus	1696
AWSDiscoveryContinuousExportFirehosePolicy	1696
Utilisation de cette stratégie	1696
Détails des politiques	1696
Version de la politique	1697
Document de stratégie JSON	1697
En savoir plus	1698
AWSDMSFleetAdvisorServiceRolePolicy	1698
Utilisation des politiques de cette politique de	1698
Détails des politiques de politique	1698
Version de la politique	1698
Document de stratégie JSON de politique	1699
En savoir plus	1699
AWSDMSServerlessServiceRolePolicy	1699
Utilisation de politique	1699
Détails des politiques	1699
Version de la politique	1700
Document de stratégie JSON	1700
En savoir plus	1701

AWSEC2CapacityReservationFleetRolePolicy	1702
Utilisation des stratégies des politiques des politiques	1702
politiques des politiques des politiques	1702
Version de la politique	1702
Document des stratégies JSON	1702
En savoir plus	1703
AWSEC2FleetServiceRolePolicy	1704
Utilisation de cette politique	1704
Les détails des politiques	1704
Version de la politique	1704
Document de stratégie JSON document de	1704
En savoir plus	1706
AWSEC2SpotFleetServiceRolePolicy	1706
Utilisation des politiques I	1707
Les politiques	1707
Version de la politique	1707
Document de stratégie JSON	1707
En savoir plus	1709
AWSEC2SpotServiceRolePolicy	1709
Utilisation de cette politique	1709
Policy details	1709
Version de la politique	1710
JSON policy document	1710
En savoir plus	1711
AWSECRPullThroughCache_ServiceRolePolicy	1711
Utilisation de cette politique	1712
Détails de la politique	1712
Version de la politique	1712
Document de politique JSON	1712
En savoir plus	1713
AWSElasticBeanstalkCustomPlatformforEC2Role	1713
Utilisation de cette stratégie	1713
Détails des politiques	1713
Version de la politique	1714
Document de stratégie JSON	1714
En savoir plus	1715

AWSElasticBeanstalkEnhancedHealth	1716
Utilisation de cette stratégie	1716
Détails des politiques	1716
Version de la politique	1716
Document de stratégie JSON	1716
En savoir plus	1717
AWSElasticBeanstalkMaintenance	1717
Utilisation de cette politique	1718
détails des politiques	1718
Version de la politique	1718
Document de stratégie JSON	1718
En savoir plus	1719
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	1719
Utilisation de cette stratégie	1719
Détails des politiques	1719
Version de la politique	1720
Document de stratégie JSON	1720
En savoir plus	1726
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	1727
utilisation une une une des politique	1727
les les les les	1727
Version de la politique	1727
un document de de	1727
En savoir plus	1733
AWSElasticBeanstalkMulticontainerDocker	1733
Utilisation de cette stratégie	1733
Détails des politiques	1733
Version de la politique	1733
Document de stratégie JSON	1733
En savoir plus	1734
AWSElasticBeanstalkReadOnly	1735
Utilisation de cette stratégie	1735
Détails de la stratégie	1735
Version de la politique	1735
Document de stratégie JSON	1735
En savoir plus	1737

AWSElasticBeanstalkRoleCore	1738
Utilisation de cette stratégie	1738
Détails des politiques	1738
Version de la politique	1738
Document de stratégie JSON	1738
En savoir plus	1743
AWSElasticBeanstalkRoleCWL	1743
Utilisation de cette stratégie	1743
Détails des politiques	1743
Version de la politique	1744
Document de stratégie JSON	1744
En savoir plus	1744
AWSElasticBeanstalkRoleECS	1745
Utilisation de cette stratégie	1745
Détails des politiques	1745
Version de la politique	1745
Document de stratégie JSON	1745
En savoir plus	1746
AWSElasticBeanstalkRoleRDS	1746
Utilisation de cette stratégie	1746
Détails des politiques	1747
Version de la politique	1747
Document de stratégie JSON	1747
En savoir plus	1748
AWSElasticBeanstalkRoleSNS	1748
Utilisation de cette stratégie	1748
Détails des politiques	1748
Version de la politique	1748
Document de stratégie JSON	1748
En savoir plus	1749
AWSElasticBeanstalkRoleWorkerTier	1749
Utilisation de cette stratégie	1750
Détails des politiques	1750
Version de la politique	1750
Document de stratégie JSON	1750
En savoir plus	1751

AWSElasticBeanstalkService	1751
Utilisation de cette stratégie	1751
Détails des politiques	1751
Version de la politique	1752
Document de stratégie JSON	1752
En savoir plus	1756
AWSElasticBeanstalkServiceRolePolicy	1756
Utilisation des des des des des des	1756
Les des politiques	1757
Version de la politique	1757
Document des politique JSON	1757
En savoir plus	1758
AWSElasticBeanstalkWebTier	1759
Utilisation de cette stratégie	1759
Détails des politiques	1759
Version de la politique	1759
Document de stratégie JSON	1759
En savoir plus	1761
AWSElasticBeanstalkWorkerTier	1761
Utilisation de cette stratégie	1761
Détails des politiques	1761
Version de la politique	1761
Document de stratégie JSON	1761
En savoir plus	1764
AWSElasticDisasterRecoveryAgentInstallationPolicy	1764
Utilisation de cette politique	1764
Détails de la politique	1764
Version de la politique	1764
Document de politique JSON	1765
En savoir plus	1766
AWSElasticDisasterRecoveryAgentPolicy	1766
Utilisation de cette politique	1766
Détails de la politique	1767
Version de la politique	1767
Document de politique JSON	1767
En savoir plus	1768

AWSElasticDisasterRecoveryConsoleFullAccess	1768
Utilisation de cette politique	1768
Détails de la politique	1768
Version de la politique	1769
Document de politique JSON	1769
En savoir plus	1778
AWSElasticDisasterRecoveryConsoleFullAccess_v2	1779
Utilisation de cette politique	1779
Détails de la politique	1779
Version de la politique	1779
Document de politique JSON	1779
En savoir plus	1792
AWSElasticDisasterRecoveryConversionServerPolicy	1792
Utilisation de cette politique	1792
Détails de la politique	1793
Version de la politique	1793
Document de politique JSON	1793
En savoir plus	1794
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	1794
Utilisation de cette politique	1794
Détails de la politique	1794
Version de la politique	1794
Document de politique JSON	1795
En savoir plus	1795
AWSElasticDisasterRecoveryEc2InstancePolicy	1796
Utilisation de cette politique	1796
Détails de la politique	1796
Version de la politique	1796
Document de politique JSON	1796
En savoir plus	1798
AWSElasticDisasterRecoveryFailbackInstallationPolicy	1798
Utilisation de cette politique	1799
Détails de la politique	1799
Version de la politique	1799
Document de politique JSON	1799
En savoir plus	1800

AWSElasticDisasterRecoveryFailbackPolicy	1800
Utilisation de cette politique	1800
Détails de la politique	1800
Version de la politique	1801
Document de politique JSON	1801
En savoir plus	1802
AWSElasticDisasterRecoveryLaunchActionsPolicy	1802
Utilisation de cette politique	1803
Détails de la politique	1803
Version de la politique	1803
Document de politique JSON	1803
En savoir plus	1809
AWSElasticDisasterRecoveryNetworkReplicationPolicy	1809
Utilisation de cette politique	1809
Détails de la politique	1809
Version de la politique	1810
Document de politique JSON	1810
En savoir plus	1811
AWSElasticDisasterRecoveryReadOnlyAccess	1811
Utilisation de cette politique	1811
Détails de la politique	1811
Version de la politique	1811
Document de politique JSON	1812
En savoir plus	1814
AWSElasticDisasterRecoveryRecoveryInstancePolicy	1814
Utilisation de cette politique	1814
Détails de la politique	1814
Version de la politique	1814
Document de politique JSON	1815
En savoir plus	1817
AWSElasticDisasterRecoveryReplicationServerPolicy	1817
Utilisation de cette politique	1818
Détails de la politique	1818
Version de la politique	1818
Document de politique JSON	1818
En savoir plus	1820

AWSElasticDisasterRecoveryServiceRolePolicy	1821
Utilisation de cette politique	1821
Détails de la politique	1821
Version de la politique	1821
Document de politique JSON	1821
En savoir plus	1830
AWSElasticDisasterRecoveryStagingAccountPolicy	1830
Utilisation de cette politique	1830
Détails de la politique	1830
Version de la politique	1830
Document de politique JSON	1831
En savoir plus	1831
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	1832
Utilisation de cette politique	1832
Détails de la politique	1832
Version de la politique	1832
Document de politique JSON	1832
En savoir plus	1833
AWSElasticLoadBalancingClassicServiceRolePolicy	1834
Utilisation de cette politique	1834
Les détails des politiques	1834
Version de la politique	1834
Document de politique JSON	1834
En savoir plus	1835
AWSElasticLoadBalancingServiceRolePolicy	1835
Utilisation cette politique politique politique politique	1835
détails des politique	1836
Version de la politique	1836
Document de stratégie JSON	1836
En savoir plus	1837
AWSElementalMediaConvertFullAccess	1837
Utilisation de cette stratégie	1837
Détails des politiques	1838
Version de la politique	1838
Document de stratégie JSON	1838
En savoir plus	1839

AWSElementalMediaConvertReadOnly	1839
Utilisation de cette stratégie	1839
Détails des politiques	1839
Version de la politique	1839
Document de stratégie JSON	1840
En savoir plus	1840
AWSElementalMediaLiveFullAccess	1840
Utilisation de cette stratégie	1840
Détails des politiques	1840
Version de la politique	1841
Document de stratégie JSON	1841
En savoir plus	1841
AWSElementalMediaLiveReadOnly	1841
Utilisation de cette stratégie	1841
Détails des politiques	1842
Version de la politique	1842
Document de stratégie JSON	1842
En savoir plus	1842
AWSElementalMediaPackageFullAccess	1843
Utilisation de cette stratégie	1843
Détails des politiques	1843
Version de la politique	1843
Document de stratégie JSON	1843
En savoir plus	1843
AWSElementalMediaPackageReadOnly	1844
Utilisation de cette stratégie	1844
Détails des politiques	1844
Version de la politique	1844
Document de stratégie JSON	1844
En savoir plus	1845
AWSElementalMediaPackageV2FullAccess	1845
Utilisation de cette politique	1845
Détails de la politique	1845
Version de la politique	1845
Document de politique JSON	1846
En savoir plus	1846

AWSElementalMediaPackageV2ReadOnly	1846
Utilisation de cette politique	1846
Détails de la politique	1846
Version de la politique	1846
Document de politique JSON	1847
En savoir plus	1847
AWSElementalMediaStoreFullAccess	1847
Utilisation de cette stratégie	1847
Détails des politiques	1847
Version de la politique	1848
Document de stratégie JSON	1848
En savoir plus	1848
AWSElementalMediaStoreReadOnly	1849
Utilisation de cette stratégie	1849
Détails des politiques	1849
Version de la politique	1849
Document de stratégie JSON	1849
En savoir plus	1850
AWSElementalMediaTailorFullAccess	1850
Utilisation de cette stratégie	1850
Détails des politiques	1850
Version de la politique	1850
Document de stratégie JSON	1851
En savoir plus	1851
AWSElementalMediaTailorReadOnly	1851
Utilisation de cette stratégie	1851
Détails des politiques	1851
Version de la politique	1852
Document de stratégie JSON	1852
En savoir plus	1852
AWSEnhancedClassicNetworkingMangementPolicy	1852
Using this policy	1852
Policy details	1853
Version de la politique	1853
JSON policy document	1853
En savoir plus	1853

AWSEntityResolutionConsoleFullAccess	1854
Utilisation de cette politique	1854
Détails de la politique	1854
Version de la politique	1854
Document de politique JSON	1854
En savoir plus	1857
AWSEntityResolutionConsoleReadOnlyAccess	1857
Utilisation de cette politique	1857
Détails de la politique	1857
Version de la politique	1858
Document de politique JSON	1858
En savoir plus	1858
AWSFaultInjectionSimulatorEC2Access	1858
Utilisation de cette politique	1859
Détails de la politique	1859
Version de la politique	1859
Document de politique JSON	1859
En savoir plus	1861
AWSFaultInjectionSimulatorECSAccess	1861
Utilisation de cette politique	1861
Détails de la politique	1861
Version de la politique	1861
Document de politique JSON	1862
En savoir plus	1863
AWSFaultInjectionSimulatorEKSAccess	1864
Utilisation de cette politique	1864
Détails de la politique	1864
Version de la politique	1864
Document de politique JSON	1864
En savoir plus	1865
AWSFaultInjectionSimulatorNetworkAccess	1866
Utilisation de cette politique	1866
Détails de la politique	1866
Version de la politique	1866
Document de politique JSON	1866
En savoir plus	1873

AWSFaultInjectionSimulatorRDSAccess	1873
Utilisation de cette politique	1874
Détails de la politique	1874
Version de la politique	1874
Document de politique JSON	1874
En savoir plus	1875
AWSFaultInjectionSimulatorSSMAccess	1875
Utilisation de cette stratégie	1876
Détails des politiques	1876
Version de la politique	1876
Document de stratégie JSON	1876
En savoir plus	1877
AWSFinSpaceServiceRolePolicy	1878
Utilisation de cette politique	1878
Détails de la politique	1878
Version de la politique	1878
Document de politique JSON	1878
En savoir plus	1879
AWSFMAdminFullAccess	1879
Utilisation de cette stratégie	1879
Détails des politiques	1879
Version de la politique	1879
Document de stratégie JSON	1880
En savoir plus	1881
AWSFMAdminReadOnlyAccess	1882
Utilisation de cette stratégie	1882
Détails des politiques	1882
Version de la politique	1882
Document de stratégie JSON	1882
En savoir plus	1884
AWSFMMemberReadOnlyAccess	1884
Utilisation de cette stratégie	1884
Détails des politiques	1884
Version de la politique	1884
Document de stratégie JSON	1885
En savoir plus	1885

AWSForWordPressPluginPolicy	1885
Utilisation de cette stratégie	1885
Détails des politiques	1885
Version de la politique	1886
Document de stratégie JSON	1886
En savoir plus	1888
AWSGitSyncServiceRolePolicy	1888
Utilisation de cette politique	1888
Détails de la politique	1888
Version de la politique	1888
Document de politique JSON	1889
En savoir plus	1889
AWSGlobalAcceleratorSLRPolicy	1889
Utilisation de cette politique	1889
Détails de la politique	1889
Version de la politique	1890
Document de politique JSON	1890
En savoir plus	1891
AWSGlueConsoleFullAccess	1892
Utilisation de cette politique	1892
Détails de la politique	1892
Version de la politique	1892
Document de politique JSON	1892
En savoir plus	1896
AWSGlueConsoleSageMakerNotebookFullAccess	1897
Utilisation de cette stratégie	1897
Détails des politiques	1897
Version de la politique	1897
Document de stratégie JSON	1897
En savoir plus	1902
AwsGlueDataBrewFullAccessPolicy	1903
Utilisation de cette stratégie	1903
Détails des politiques	1903
Version de la politique	1903
Document de stratégie JSON	1903
En savoir plus	1908

AWSGlueDataBrewServiceRole	1909
Utilisation de cette politique	1909
Détails de la politique	1909
Version de la politique	1909
Document de politique JSON	1909
En savoir plus	1912
AWSGlueSchemaRegistryFullAccess	1912
Utilisation de cette stratégie	1912
Détails des stratégies	1912
Version de la politique	1913
Document de stratégie JSON	1913
En savoir plus	1914
AWSGlueSchemaRegistryReadOnlyAccess	1914
Utilisation de cette stratégie	1914
Détails de la stratégie	1915
Version de la politique	1915
Document de stratégie JSON	1915
En savoir plus	1916
AWSGlueServiceNotebookRole	1916
Utilisation de cette politique	1916
Détails de la politique	1916
Version de la politique	1916
Document de politique JSON	1916
En savoir plus	1919
AWSGlueServiceRole	1919
Utilisation de cette politique	1919
Détails de la politique	1919
Version de la politique	1919
Document de politique JSON	1920
En savoir plus	1922
AwsGlueSessionUserRestrictedNotebookPolicy	1922
Utilisation de cette politique	1922
Détails de la politique	1922
Version de la politique	1923
Document de politique JSON	1923
En savoir plus	1925

AwsGlueSessionUserRestrictedNotebookServiceRole	1925
Utilisation de cette politique.	1926
Détails des détails de détails	1926
Version de la politique	1926
Document de de de stratégie JSON	1926
En savoir plus	1930
AwsGlueSessionUserRestrictedPolicy	1930
Utilisation de cette politique	1930
Détails des politiques	1930
Version de la politique	1931
Document de stratégie JSON	1931
En savoir plus	1933
AwsGlueSessionUserRestrictedServiceRole	1933
Utilisation de cette politique de politique de	1933
Détails de la politique de	1933
Version de la politique	1934
Document de stratégie de stratégie de stratégie	1934
En savoir plus	1937
AWSGrafanaAccountAdministrator	1938
Utilisation de cette stratégie	1938
Détails des politiques	1938
Version de la politique	1938
Document de stratégie JSON	1938
En savoir plus	1939
AWSGrafanaConsoleReadOnlyAccess	1939
Utilisation de cette stratégie	1940
Détails des politiques	1940
Version de la politique	1940
Document de stratégie JSON	1940
En savoir plus	1941
AWSGrafanaWorkspacePermissionManagement	1941
Utilisation de cette stratégie	1941
Détails des politiques	1941
Version de la politique	1941
Document de stratégie JSON	1941
En savoir plus	1942

AWSGrafanaWorkspacePermissionManagementV2	1943
Utilisation de cette politique	1943
Détails de la politique	1943
Version de la politique	1943
Document de politique JSON	1943
En savoir plus	1944
AWSGreengrassFullAccess	1944
Utilisation de cette stratégie	1944
Détails des politiques	1945
Version de la politique	1945
Document de politique JSON	1945
En savoir plus	1945
AWSGreengrassReadOnlyAccess	1946
Utilisation de cette stratégie	1946
Détails des politiques	1946
Version de la politique	1946
Document de stratégie JSON	1946
En savoir plus	1947
AWSGreengrassResourceAccessRolePolicy	1947
Utilisation de cette stratégie	1947
Détails des politiques	1947
Version de la politique	1947
Document de stratégie JSON	1948
En savoir plus	1950
AWSGroundStationAgentInstancePolicy	1950
Utilisation de cette stratégie	1950
Détails des politiques	1950
Version de la politique	1951
Document de stratégie JSON	1951
En savoir plus	1951
AWSHealth_EventProcessorServiceRolePolicy	1951
Utilisation de cette politique	1952
Les détails des politiques	1952
Version de la politique	1952
Document de stratégie JSON	1952
En savoir plus	1953

AWSHealthFullAccess	1953
Utilisation de cette politique	1953
Détails des politiques	1953
Version de la politique	1953
Document de stratégie JSON	1954
En savoir plus	1955
AWSHealthImagingFullAccess	1955
Utilisation de cette politique	1955
Détails de la politique	1955
Version de la politique	1955
Document de politique JSON	1955
En savoir plus	1956
AWSHealthImagingReadOnlyAccess	1956
Utilisation de cette politique	1956
Détails de la politique	1957
Version de la politique	1957
Document de politique JSON	1957
En savoir plus	1958
AWSIAMIdentityCenterAllowListForIdentityContext	1958
Utilisation de cette politique	1958
Détails de la politique	1958
Version de la politique	1958
Document de politique JSON	1959
En savoir plus	1960
AWSIdentitySyncFullAccess	1961
Utilisation de cette stratégie	1961
Détails des politiques	1961
Version de la politique	1961
Document de stratégie JSON	1961
En savoir plus	1962
AWSIdentitySyncReadOnlyAccess	1962
Utilisation de cette stratégie	1962
Détails des politiques	1962
Version de la politique	1963
Document de stratégie JSON	1963
En savoir plus	1963

AWSImageBuilderFullAccess	1963
Utilisation de cette stratégie	1964
Détails des stratégies	1964
Version de la politique	1964
Document de stratégie JSON	1964
En savoir plus	1967
AWSImageBuilderReadOnlyAccess	1967
Utilisation de cette stratégie	1967
Détails des politiques	1967
Version de la politique	1967
Document de stratégie JSON	1968
En savoir plus	1968
AWSImportExportFullAccess	1968
Utilisation de cette stratégie	1968
Détails des politiques	1969
Version de la politique	1969
Document de stratégie JSON	1969
En savoir plus	1969
AWSImportExportReadOnlyAccess	1970
Utilisation de cette stratégie	1970
Détails des politiques	1970
Version de la politique	1970
Document de stratégie JSON	1970
En savoir plus	1971
AWSIncidentManagerIncidentAccessServiceRolePolicy	1971
Utilisation de cette politique	1971
Détails de la politique	1971
Version de la politique	1971
Document de politique JSON	1972
En savoir plus	1972
AWSIncidentManagerResolverAccess	1972
Utilisation de cette stratégie	1972
Détails des politiques	1973
Version de la politique	1973
Document de stratégie JSON	1973
En savoir plus	1974

AWSIncidentManagerServiceRolePolicy	1974
Utilisation de cette politique	1974
Les détails des politiques	1974
Version de la politique	1975
Document de stratégie JSON	1975
En savoir plus	1976
AWSIoT1ClickFullAccess	1976
Utilisation de cette stratégie	1976
Détails des politiques	1976
Version de la politique	1977
Document de stratégie JSON	1977
En savoir plus	1977
AWSIoT1ClickReadOnlyAccess	1977
Utilisation de cette stratégie	1977
Détails des politiques	1978
Version de la politique	1978
Document de stratégie JSON	1978
En savoir plus	1978
AWSIoTAnalyticsFullAccess	1979
Utilisation de cette stratégie	1979
Détails des politiques	1979
Version de la politique	1979
Document de stratégie JSON	1979
En savoir plus	1980
AWSIoTAnalyticsReadOnlyAccess	1980
Utilisation de cette stratégie	1980
Détails des politiques	1980
Version de la politique	1980
Document de stratégie JSON	1980
En savoir plus	1981
AWSIoTConfigAccess	1981
Utilisation de cette stratégie	1981
Détails des politiques	1981
Version de la politique	1981
Document de stratégie JSON	1982
En savoir plus	1985

AWSIoTConfigReadOnlyAccess	1986
Utilisation de cette stratégie	1986
Détails des politiques	1986
Version de la politique	1986
Document de stratégie JSON	1986
En savoir plus	1988
AWSIoTDataAccess	1988
Utilisation de cette stratégie	1989
Détails des politiques	1989
Version de la politique	1989
Document de stratégie JSON	1989
En savoir plus	1990
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	1990
Utilisation de cette stratégie	1990
Détails des politiques	1990
Version de la politique	1990
Document de stratégie JSON	1991
En savoir plus	1991
AWSIoTDeviceDefenderAudit	1991
Utilisation de cette stratégie	1991
Détails des politiques	1991
Version de la politique	1992
Document de stratégie JSON	1992
En savoir plus	1993
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	1993
Utilisation de cette stratégie	1993
Détails des politiques	1993
Version de la politique	1993
Document de stratégie JSON	1994
En savoir plus	1994
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	1995
Utilisation de cette stratégie	1995
Détails des politiques	1995
Version de la politique	1995
Document de stratégie JSON	1995
En savoir plus	1996

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	1996
Utilisation de cette stratégie	1996
Détails des politiques	1996
Version de la politique	1997
Document de stratégie JSON	1997
En savoir plus	1997
AWSIoTDeviceDefenderUpdateCACertMitigationAction	1997
Utilisation de cette stratégie	1998
Détails des politiques	1998
Version de la politique	1998
Document de stratégie JSON	1998
En savoir plus	1999
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	1999
Utilisation de cette stratégie	1999
Détails des politiques	1999
Version de la politique	1999
Document de stratégie JSON	1999
En savoir plus	2000
AWSIoTDeviceTesterForFreeRTOSFullAccess	2000
Utilisation de cette politique	2000
Détails de la politique	2000
Version de la politique	2001
Document de politique JSON	2001
En savoir plus	2007
AWSIoTDeviceTesterForGreengrassFullAccess	2007
Utilisation de cette stratégie	2007
Détails des politiques	2007
Version de la politique	2008
Document de stratégie JSON	2008
En savoir plus	2011
AWSIoTEventsFullAccess	2011
Utilisation de cette stratégie	2011
Détails des politiques	2011
Version de la politique	2011
Document de stratégie JSON	2011
En savoir plus	2012

AWSIoTEventsReadOnlyAccess	2012
Utilisation de cette stratégie	2012
Détails des politiques	2012
Version de la politique	2012
Document de stratégie JSON	2013
En savoir plus	2013
AWSIoTFleetHubFederationAccess	2013
Utilisation de cette stratégie	2013
Détails des politiques	2014
Version de la politique	2014
Document de stratégie JSON	2014
En savoir plus	2016
AWSIoTFleetwiseServiceRolePolicy	2016
Utilisation de cette politique	2016
Les détails des politiques	2016
Version de la politique	2016
Document de stratégie JSON	2017
En savoir plus	2017
AWSIoTFullAccess	2017
Utilisation de cette stratégie	2017
Détails des politiques	2018
Version de la politique	2018
Document de stratégie JSON	2018
En savoir plus	2018
AWSIoTLogging	2019
Utilisation de cette stratégie	2019
Détails des politiques	2019
Version de la politique	2019
Document de stratégie JSON	2019
En savoir plus	2020
AWSIoTOTAUpdate	2020
Utilisation de cette stratégie	2020
Détails des politiques	2020
Version de la politique	2020
Document de stratégie JSON	2021
En savoir plus	2021

AWSIoTRoboRunnerFullAccess	2021
Utilisation de cette stratégie	2021
Détails des politiques	2021
Version de la politique	2022
Document de stratégie JSON	2022
En savoir plus	2022
AWSIoTRoboRunnerReadOnly	2023
Utilisation de cette stratégie	2023
Détails des politiques	2023
Version de la politique	2023
Document de stratégie JSON	2023
En savoir plus	2024
AWSIoTRoboRunnerServiceRolePolicy	2024
Utilisation de politique	2024
détails des politique	2024
Version de la politique	2024
Document stratégie JSON	2025
En savoir plus	2025
AWSIoTRuleActions	2025
Utilisation de cette stratégie	2025
Détails des politiques	2026
Version de la politique	2026
Document de stratégie JSON	2026
En savoir plus	2026
AWSIoTSiteWiseConsoleFullAccess	2027
Utilisation de cette stratégie	2027
Détails des politiques	2027
Version de la politique	2027
Document de stratégie JSON	2027
En savoir plus	2030
AWSIoTSiteWiseFullAccess	2030
Utilisation de cette stratégie	2030
Détails des politiques	2030
Version de la politique	2030
Document de stratégie JSON	2030
En savoir plus	2031

AWSIoTSiteWiseMonitorPortalAccess	2031
Utilisation de cette stratégie	2031
Détails des politiques	2031
Version de la politique	2032
Document de stratégie JSON	2032
En savoir plus	2033
AWSIoTSiteWiseMonitorServiceRolePolicy	2033
Utilisation des stratégies de stratégies de politiques	2033
Les détails des politiques	2033
Version de la politique	2033
Document de stratégie JSON document de	2034
En savoir plus	2035
AWSIoTSiteWiseReadOnlyAccess	2035
Utilisation de cette stratégie	2035
Détails des politiques	2035
Version de la politique	2035
Document de stratégie JSON	2035
En savoir plus	2036
AWSIoTThingsRegistration	2036
Utilisation de cette stratégie	2036
Détails des politiques	2036
Version de la politique	2037
Document de politique JSON	2037
En savoir plus	2038
AWSIoTThingMakerServiceRolePolicy	2038
Utilisation de cette politique	2038
Détails de la politique	2038
Version de la politique	2039
Document de politique JSON	2039
En savoir plus	2040
AWSIoTWirelessDataAccess	2040
Utilisation de cette stratégie	2041
Détails des politiques	2041
Version de la politique	2041
Document de stratégie JSON	2041
En savoir plus	2041

AWSIoTWirelessFullAccess	2042
Utilisation de cette stratégie	2042
Détails des politiques	2042
Version de la politique	2042
Document de stratégie JSON	2042
En savoir plus	2043
AWSIoTWirelessFullPublishAccess	2043
Utilisation de cette stratégie	2043
Détails des politiques	2043
Version de la politique	2043
Document de stratégie JSON	2044
En savoir plus	2044
AWSIoTWirelessGatewayCertManager	2044
Utilisation de cette stratégie	2044
Détails des politiques	2044
Version de la politique	2045
Document de stratégie JSON	2045
En savoir plus	2045
AWSIoTWirelessLogging	2046
Utilisation de cette stratégie	2046
Détails des politiques	2046
Version de la politique	2046
Document de stratégie JSON	2046
En savoir plus	2047
AWSIoTWirelessReadOnlyAccess	2047
Utilisation de cette stratégie	2047
Détails des politiques	2047
Version de la politique	2047
Document de stratégie JSON	2048
En savoir plus	2048
AWSIPAMServiceRolePolicy	2048
Utilisation de cette politique	2048
Détails de la politique	2048
Version de la politique	2049
Document de politique JSON	2049
En savoir plus	2050

AWSIQContractServiceRolePolicy	2050
utilisation des politique	2050
les détails des politique	2050
Version de la politique	2051
document des politique JSON	2051
En savoir plus	2051
AWSIQFullAccess	2051
Utilisation de cette stratégie	2051
Détails des politiques	2051
Version de la politique	2052
Document de stratégie JSON	2052
En savoir plus	2053
AWSIQPermissionServiceRolePolicy	2053
Utilisation des de cette politique	2053
Les détails des politiques	2053
Version de la politique	2053
Document de stratégie JSON	2053
En savoir plus	2054
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2055
Utilisation de cette politique	2055
Détails de la politique	2055
Version de la politique	2055
Document de politique JSON	2055
En savoir plus	2056
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2056
Utilisation de cette politique	2056
Utilisation des politiques	2056
Version de la politique	2056
Document de stratégie JSON	2057
En savoir plus	2057
AWSKeyManagementServicePowerUser	2057
Utilisation de cette stratégie	2057
Détails des politiques	2057
Version de la politique	2058
Document de stratégie JSON	2058
En savoir plus	2058

AWSLakeFormationCrossAccountManager	2059
Utilisation de cette politique	2059
Détails de la politique	2059
Version de la politique	2059
Document de politique JSON	2059
En savoir plus	2061
AWSLakeFormationDataAdmin	2061
Utilisation de cette stratégie	2061
Détails des politiques	2062
Version de la politique	2062
Document de stratégie JSON	2062
En savoir plus	2063
AWSLambda_FullAccess	2063
Utilisation de cette stratégie	2064
Détails des politiques	2064
Version de la politique	2064
Document de stratégie JSON	2064
En savoir plus	2065
AWSLambda_ReadOnlyAccess	2066
Utilisation de cette politique	2066
Détails de la politique	2066
Version de la politique	2066
Document de politique JSON	2066
En savoir plus	2067
AWSLambdaBasicExecutionRole	2068
Utilisation de cette stratégie	2068
Détails des politiques	2068
Version de la politique	2068
Document de stratégie JSON	2068
En savoir plus	2069
AWSLambdaDynamoDBExecutionRole	2069
Utilisation de cette stratégie	2069
Détails des politiques	2069
Version de la politique	2069
Document de stratégie JSON	2070
En savoir plus	2070

AWSLambdaENIManagementAccess	2070
Utilisation de cette stratégie	2070
Détails des politiques	2071
Version de la politique	2071
Document de stratégie JSON	2071
En savoir plus	2071
AWSLambdaExecute	2072
Utilisation de cette stratégie	2072
Détails des politiques	2072
Version de la politique	2072
Document de stratégie JSON	2072
En savoir plus	2073
AWSLambdaFullAccess	2073
Utilisation de cette stratégie	2073
Détails des politiques	2073
Version de la politique	2074
Document de stratégie JSON	2074
En savoir plus	2075
AWSLambdaInvocation-DynamoDB	2076
Utilisation de cette stratégie	2076
Détails des politiques	2076
Version de la politique	2076
Document de stratégie JSON	2076
En savoir plus	2077
AWSLambdaKinesisExecutionRole	2077
Utilisation de cette stratégie	2077
Détails des politiques	2077
Version de la politique	2077
Document de stratégie JSON	2078
En savoir plus	2078
AWSLambdaMSKExecutionRole	2079
Utilisation de cette stratégie	2079
Détails des politiques	2079
Version de la politique	2079
Document de stratégie JSON	2079
En savoir plus	2080

AWSLambdaReplicator	2080
Utilisation de cette politique	2080
Les détails des politiques	2080
Version de la politique	2081
Document de stratégie JSON	2081
En savoir plus	2082
AWSLambdaRole	2082
Utilisation de cette stratégie	2082
Détails des politiques	2082
Version de la politique	2082
Document de stratégie JSON	2083
En savoir plus	2083
AWSLambdaSQSQueueExecutionRole	2083
Utilisation de cette stratégie	2083
Détails des politiques	2083
Version de la politique	2084
Document de stratégie JSON	2084
En savoir plus	2084
AWSLambdaVPCLambdaAccessExecutionRole	2085
Utilisation de cette politique	2085
Détails de la politique	2085
Version de la politique	2085
Document de politique JSON	2085
En savoir plus	2086
AWSLicenseManagerConsumptionPolicy	2086
Utilisation de cette stratégie	2086
Détails des politiques	2086
Version de la politique	2087
Document de stratégie JSON	2087
En savoir plus	2087
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	2087
Utilisation de cette politique	2088
Les détails des politiques	2088
Version de la politique	2088
Document de stratégie JSON	2088
En savoir plus	2089

AWSLicenseManagerMasterAccountRolePolicy	2089
Utilisation de de de de cette politique	2089
Les détails des des des	2089
Version de la politique	2090
Document de de de de de la	2090
En savoir plus	2095
AWSLicenseManagerMemberAccountRolePolicy	2095
Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation	2095
détails	2095
Version de la politique	2095
Document politique JSON	2095
En savoir plus	2097
AWSLicenseManagerServiceRolePolicy	2097
Utilisation de cette politique	2097
Détails des politiques	2097
Version de la politique	2097
Document de politique JSON	2097
En savoir plus	2101
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	2101
Utilisation de cette politique	2101
Les détails des politiques	2101
Version de la politique	2101
Document de stratégie JSON	2101
En savoir plus	2103
AWSM2ServicePolicy	2104
Utilisation des stratégies IAM	2104
Les détails des politiques	2104
Version de la politique	2104
Document de stratégies JSON	2104
En savoir plus	2106
AWSManagedServices_ContactsServiceRolePolicy	2106
Utilisation de stratégies	2106
Les politiques	2106
Version de la politique	2106
politique JSON	2106
En savoir plus	2107

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	2107
Utilisation de cette politique des politiques politiques	2107
Les détails des politiques politiques	2108
Version de la politique	2108
Document de stratégie JSON des politiques	2108
En savoir plus	2109
AWSManagedServices_EventsServiceRolePolicy	2110
Utilisation de cette politique	2110
Les détails des politiques	2110
Version de la politique	2110
Document de stratégie JSON	2110
En savoir plus	2111
AWSManagedServicesDeploymentToolkitPolicy	2111
Utilisation de politiques de politique de politique	2111
Détails des politiques	2111
Version de la politique	2112
Document de stratégie JSON document de	2112
En savoir plus	2114
AWSMarketplaceAmilngestion	2114
Utilisation de cette stratégie	2114
Détails des politiques	2114
Version de la politique	2115
Document de stratégie JSON	2115
En savoir plus	2115
AWSMarketplaceDeploymentServiceRolePolicy	2116
Utilisation de cette politique	2116
Détails de la politique	2116
Version de la politique	2116
Document de politique JSON	2116
En savoir plus	2118
AWSMarketplaceFullAccess	2118
Utilisation de cette stratégie	2118
Détails des politiques	2118
Version de la politique	2118
Document de stratégie JSON	2118
En savoir plus	2122

AWSMarketplaceGetEntitlements	2122
Utilisation de cette stratégie	2122
Détails des politiques	2122
Version de la politique	2122
Document de stratégie JSON	2122
En savoir plus	2123
AWSMarketplaceImageBuildFullAccess	2123
Utilisation de cette stratégie	2123
Détails des politiques	2123
Version de la politique	2124
Document de stratégie JSON	2124
En savoir plus	2127
AWSMarketplaceLicenseManagementServiceRolePolicy	2128
Utilisation de stratégies Utilisation de stratégies Utilisation	2128
détails des politiques de politique	2128
Version de la politique	2128
document de stratégie JSON, document	2128
En savoir plus	2129
AWSMarketplaceManageSubscriptions	2129
Utilisation de cette stratégie	2129
Détails des politiques	2129
Version de la politique	2130
Document de stratégie JSON	2130
En savoir plus	2131
AWSMarketplaceMeteringFullAccess	2131
Utilisation de cette stratégie	2131
Détails des politiques	2131
Version de la politique	2131
Document de stratégie JSON	2131
En savoir plus	2132
AWSMarketplaceMeteringRegisterUsage	2132
Utilisation de cette stratégie	2132
Détails des politiques	2132
Version de la politique	2133
Document de stratégie JSON	2133
En savoir plus	2133

AWSMarketplaceProcurementSystemAdminFullAccess	2133
Utilisation de cette stratégie	2134
Détails des politiques	2134
Version de la politique	2134
Document de stratégie JSON	2134
En savoir plus	2135
AWSMarketplacePurchaseOrdersServiceRolePolicy	2135
Utilisation des politiques	2135
Les détails des politiques	2135
Version de la politique	2135
Document de stratégie JSON	2136
En savoir plus	2136
AWSMarketplaceRead-only	2136
Utilisation de cette stratégie	2136
Détails des politiques	2136
Version de la politique	2137
Document de stratégie JSON	2137
En savoir plus	2138
AWSMarketplaceResaleAuthorizationServiceRolePolicy	2138
Utilisation de cette politique	2138
Détails de la politique	2138
Version de la politique	2139
Document de politique JSON	2139
En savoir plus	2141
AWSMarketplaceSellerFullAccess	2141
Utilisation de cette politique	2141
Détails de la politique	2142
Version de la politique	2142
Document de politique JSON	2142
En savoir plus	2145
AWSMarketplaceSellerProductsFullAccess	2146
Utilisation de cette politique	2146
Détails de la politique	2146
Version de la politique	2146
Document de politique JSON	2146
En savoir plus	2148

AWSMarketplaceSellerProductsReadOnly	2148
Utilisation de cette stratégie	2148
Détails des politiques	2148
Version de la politique	2149
Document de stratégie JSON	2149
En savoir plus	2150
AWSMediaConnectServicePolicy	2150
Utilisation des stratégies Utilisation des politiques Utilisation	2150
détails des détails des politiques	2150
Version de la politique	2150
Document de stratégie JSON	2150
En savoir plus	2152
AWSMediaTailorServiceRolePolicy	2152
Utilisation de cette politique	2152
Les détails des politiques	2152
Version de la politique	2152
Document de stratégie JSON	2153
En savoir plus	2153
AWSMigrationHubDiscoveryAccess	2153
Utilisation de cette stratégie	2153
Détails des politiques	2154
Version de la politique	2154
Document de stratégie JSON	2154
En savoir plus	2155
AWSMigrationHubDMSAccess	2155
Utilisation de cette stratégie	2156
Détails des politiques	2156
Version de la politique	2156
Document de stratégie JSON	2156
En savoir plus	2157
AWSMigrationHubFullAccess	2157
Utilisation de cette stratégie	2157
Détails des politiques	2157
Version de la politique	2158
Document de stratégie JSON	2158
En savoir plus	2159

AWSMigrationHubOrchestratorConsoleFullAccess	2159
Utilisation de cette politique	2160
Détails de la politique	2160
Version de la politique	2160
Document de politique JSON	2160
En savoir plus	2163
AWSMigrationHubOrchestratorInstanceRolePolicy	2163
Utilisation de cette stratégie	2164
Détails des politiques	2164
Version de la politique	2164
Document de stratégie JSON	2164
En savoir plus	2165
AWSMigrationHubOrchestratorPlugin	2165
Utilisation de cette stratégie	2165
Détails des politiques	2165
Version de la politique	2165
Document de stratégie JSON	2166
En savoir plus	2167
AWSMigrationHubOrchestratorServiceRolePolicy	2167
Utilisation de cette politique	2167
Détails de la politique	2167
Version de la politique	2168
Document de politique JSON	2168
En savoir plus	2171
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	2171
Utilisation de cette politique	2172
Détails de la politique	2172
Version de la politique	2172
Document de politique JSON	2172
En savoir plus	2177
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	2177
Utilisation de cette politique	2178
Détails de la politique	2178
Version de la politique	2178
Document de politique JSON	2178
En savoir plus	2180

AWSMigrationHubRefactorSpacesFullAccess	2180
Utilisation de cette politique	2180
Détails de la politique	2180
Version de la politique	2180
Document de politique JSON	2181
En savoir plus	2186
AWSMigrationHubRefactorSpacesServiceRolePolicy	2187
Utilisation de cette politique	2187
Détails de la politique	2187
Version de la politique	2187
Document de politique JSON	2187
En savoir plus	2191
AWSMigrationHubSMSAccess	2191
Utilisation de cette stratégie	2191
Détails des politiques	2191
Version de la politique	2192
Document de stratégie JSON	2192
En savoir plus	2193
AWSMigrationHubStrategyCollector	2193
Utilisation de cette politique	2193
Détails de la politique	2193
Version de la politique	2193
Document de politique JSON	2194
En savoir plus	2196
AWSMigrationHubStrategyConsoleFullAccess	2196
Utilisation de cette stratégie	2196
Détails des politiques	2196
Version de la politique	2196
Document de stratégie JSON	2197
En savoir plus	2198
AWSMigrationHubStrategyServiceRolePolicy	2199
Utilisation de politique de politique de politique	2199
détails des politiques de politique	2199
Version de la politique	2199
Document de stratégie JSON	2199
En savoir plus	2200

AWSMobileHub_FullAccess	2200
Utilisation de cette stratégie	2201
Détails des politiques	2201
Version de la politique	2201
Document de stratégie JSON	2201
En savoir plus	2203
AWSMobileHub_ReadOnly	2203
Utilisation de cette stratégie	2203
Détails des politiques	2203
Version de la politique	2203
Document de stratégie JSON	2203
En savoir plus	2205
AWSMSKReplicatorExecutionRole	2205
Utilisation de cette politique	2205
Détails de la politique	2205
Version de la politique	2205
Document de politique JSON	2205
En savoir plus	2207
AWSNetworkFirewallServiceRolePolicy	2207
Utilisation de cette politique	2207
Les détails des politiques	2207
Version de la politique	2208
Document de stratégie JSON	2208
En savoir plus	2209
AWSNetworkManagerCloudWANServiceRolePolicy	2209
Utilisation	2210
Détails	2210
Version de la politique	2210
Document JSON	2210
En savoir plus	2211
AWSNetworkManagerFullAccess	2211
Utilisation de cette stratégie	2211
Détails des politiques	2211
Version de la politique	2211
Document de stratégie JSON	2211
En savoir plus	2212

AWSNetworkManagerReadOnlyAccess	2212
Utilisation de cette stratégie	2212
Détails des politiques	2212
Version de la politique	2213
Document de stratégie JSON	2213
En savoir plus	2213
AWSNetworkManagerServiceRolePolicy	2213
Utilisation	2214
les les les les les	2214
Version de la politique	2214
Document de politique JSON	2214
En savoir plus	2215
AWSOpsWorks_FullAccess	2215
Utilisation de cette stratégie	2215
Détails de la stratégie	2215
Version de la politique	2216
Document de stratégie JSON	2216
En savoir plus	2217
AWSOpsWorksCloudWatchLogs	2217
Utilisation de la présente stratégie	2217
Détails des politiques	2217
Version de la politique	2218
Document de stratégie JSON	2218
En savoir plus	2218
AWSOpsWorksCMInstanceProfileRole	2218
Utilisation de cette stratégie	2219
Détails des politiques	2219
Version de la politique	2219
Document de stratégie JSON	2219
En savoir plus	2220
AWSOpsWorksCMServiceRole	2220
Utilisation de cette stratégie	2220
Détails des politiques	2220
Version de la politique	2221
Document de stratégie JSON	2221
En savoir plus	2225

AWSOpsWorksInstanceRegistration	2225
Utilisation de cette stratégie	2225
Détails des politiques	2225
Version de la politique	2226
Document de stratégie JSON	2226
En savoir plus	2226
AWSOpsWorksRegisterCLI_EC2	2227
Utilisation de cette stratégie	2227
Détails de la stratégie	2227
Version de la politique	2227
Document de stratégie JSON	2227
En savoir plus	2228
AWSOpsWorksRegisterCLI_OnPremises	2228
Utilisation de cette stratégie	2228
Détails de la stratégie	2228
Version de la politique	2229
Document de stratégie JSON	2229
En savoir plus	2230
AWSOrganizationsFullAccess	2231
Utilisation de cette politique	2231
Détails de la politique	2231
Version de la politique	2231
Document de politique JSON	2231
En savoir plus	2232
AWSOrganizationsReadOnlyAccess	2232
Utilisation de cette politique	2232
Détails de la politique	2233
Version de la politique	2233
Document de politique JSON	2233
En savoir plus	2234
AWSOrganizationsServiceTrustPolicy	2234
Utilisation de cette politique	2234
Les détails des politiques	2234
Version de la politique	2234
Document de stratégie JAM	2235
En savoir plus	2235

AWSOutpostsAuthorizeServerPolicy	2235
Utilisation de cette stratégie	2235
Détails des politiques	2236
Version de la politique	2236
Document de stratégie JSON	2236
En savoir plus	2236
AWSOutpostsServiceRolePolicy	2237
Utilisation de cette politique	2237
Les détails des politiques	2237
Version de la politique	2237
Document de stratégie JSON	2237
En savoir plus	2238
AWSPanoramaApplianceRolePolicy	2238
Utilisation de cette stratégie	2238
Détails des politiques	2238
Version de la politique	2238
Document de stratégie JSON	2238
En savoir plus	2239
AWSPanoramaApplianceServiceRolePolicy	2239
Utilisation de cette stratégie	2239
Détails des politiques	2240
Version de la politique	2240
Document de stratégie JSON	2240
En savoir plus	2241
AWSPanoramaFullAccess	2242
Utilisation de cette stratégie	2242
Détails des politiques	2242
Version de la politique	2242
Document de stratégie JSON	2242
En savoir plus	2245
AWSPanoramaGreengrassGroupRolePolicy	2245
Utilisation de cette stratégie	2245
Détails des politiques	2245
Version de la politique	2245
Document de stratégie JSON	2246
En savoir plus	2247

AWSPanoramaSageMakerRolePolicy	2247
Utilisation de cette stratégie	2247
Détails des politiques	2247
Version de la politique	2248
Document de stratégie JSON	2248
En savoir plus	2248
AWSPanoramaServiceLinkedRolePolicy	2248
Utilisation de cette politique	2249
Les détails des politiques	2249
Version de la politique	2249
Document de stratégie JSON	2249
En savoir plus	2252
AWSPanoramaServiceRolePolicy	2252
Utilisation de cette stratégie	2252
Détails des politiques	2252
Version de la politique	2252
Document de stratégie JSON	2253
En savoir plus	2259
AWSPriceListServiceFullAccess	2260
Utilisation de cette stratégie	2260
Détails des politiques	2260
Version de la politique	2260
Document de stratégie JSON	2260
En savoir plus	2261
AWSPrivateCAAuditor	2261
Utilisation de cette stratégie	2261
Détails des politiques	2261
Version de la politique	2261
Document de stratégie JSON	2261
En savoir plus	2262
AWSPrivateCAFullAccess	2262
Utilisation de cette stratégie	2263
Détails des politiques	2263
Version de la politique	2263
Document de stratégie JSON	2263
En savoir plus	2263

AWSPriateCAPrivilegedUser	2264
Utilisation de cette stratégie	2264
Détails des politiques	2264
Version de la politique	2264
Document de stratégie JSON	2264
En savoir plus	2265
AWSPriateCAReadOnly	2266
Utilisation de cette stratégie	2266
Détails des politiques	2266
Version de la politique	2266
Document de stratégie JSON	2266
En savoir plus	2267
AWSPriateCAUser	2267
Utilisation de cette stratégie	2267
Détails des politiques	2267
Version de la politique	2267
Document de stratégie JSON	2268
En savoir plus	2269
AWSPriateMarketplaceAdminFullAccess	2269
Utilisation de cette politique	2269
Détails de la politique	2269
Version de la politique	2270
Document de politique JSON	2270
En savoir plus	2271
AWSPriateMarketplaceRequests	2271
Utilisation de cette stratégie	2272
Détails des politiques	2272
Version de la politique	2272
Document de stratégie JSON	2272
En savoir plus	2272
AWSPriateNetworksServiceRolePolicy	2273
Utilisation de cette politique	2273
Les détails des politiques	2273
Version de la politique	2273
Document de stratégie JSON	2273
En savoir plus	2274

AWSProtonCodeBuildProvisioningBasicAccess	2274
Utilisation de cette stratégie	2274
Détails des politiques	2274
Version de la politique	2274
Document de stratégie JSON	2275
En savoir plus	2275
AWSProtonCodeBuildProvisioningServiceRolePolicy	2276
Utilisation de politique de politique de politique	2276
Détails des politiques de politique	2276
Version de la politique	2276
Document de politique JSON Document de	2276
En savoir plus	2278
AWSProtonDeveloperAccess	2278
Utilisation de cette stratégie	2278
Détails des politiques	2278
Version de la politique	2278
Document de stratégie JSON	2278
En savoir plus	2280
AWSProtonFullAccess	2281
Utilisation de cette stratégie	2281
Détails des politiques	2281
Version de la politique	2281
Document de stratégie JSON	2281
En savoir plus	2283
AWSProtonReadOnlyAccess	2283
Utilisation de cette stratégie	2283
Détails des politiques	2283
Version de la politique	2283
Document de stratégie JSON	2284
En savoir plus	2285
AWSProtonServiceGitSyncServiceRolePolicy	2285
Utilisation de cette politique	2285
Détails des politiques	2286
Version de la politique	2286
Document de stratégie JSON	2286
En savoir plus	2287

AWSProtonSyncServiceRolePolicy	2287
Utilisation des stratégies politiques des stratégies	2287
Utilisation des politiques des politiques	2287
Version de la politique	2287
Document de stratégies JSON	2288
En savoir plus	2289
AWSPurchaseOrdersServiceRolePolicy	2289
Utilisation de cette politique	2289
Détails de la politique	2289
Version de la politique	2289
Document de politique JSON	2289
En savoir plus	2290
AWSQuicksightAthenaAccess	2290
Utilisation de cette stratégie	2291
Détails des politiques	2291
Version de la politique	2291
Document de stratégie JSON	2291
En savoir plus	2293
AWSQuickSightDescribeRDS	2294
Utilisation de cette stratégie	2294
Détails des politiques	2294
Version de la politique	2294
Document de stratégie JSON	2294
En savoir plus	2295
AWSQuickSightDescribeRedshift	2295
Utilisation de cette stratégie	2295
Détails des politiques	2295
Version de la politique	2295
Document de stratégie JSON	2295
En savoir plus	2296
AWSQuickSightElasticsearchPolicy	2296
Utilisation de cette stratégie	2296
Détails des politiques	2296
Version de la politique	2296
Document de stratégie JSON	2297
En savoir plus	2298

AWSQuickSightIoTAnalyticsAccess	2298
Utilisation de cette stratégie	2298
Détails des politiques	2298
Version de la politique	2298
Document de stratégie JSON	2299
En savoir plus	2299
AWSQuickSightListIAM	2299
Utilisation de cette stratégie	2299
Détails des politiques	2299
Version de la politique	2300
Document de stratégie JSON	2300
En savoir plus	2300
AWSQuickSightOpenSearchPolicy	2300
Utilisation de cette stratégie	2301
Détails des politiques	2301
Version de la politique	2301
Document de stratégie JSON	2301
En savoir plus	2302
AWSQuickSightSageMakerPolicy	2302
Utilisation de cette politique	2302
Détails de la politique	2303
Version de la politique	2303
Document de politique JSON	2303
En savoir plus	2304
AWSQuickSightTimestreamPolicy	2304
Utilisation de cette stratégie	2305
Détails des politiques	2305
Version de la politique	2305
Document de stratégie JSON	2305
En savoir plus	2306
AWSReachabilityAnalyzerServiceRolePolicy	2306
Utilisation de cette politique	2306
Détails de la politique	2306
Version de la politique	2306
Document de politique JSON	2307
En savoir plus	2309

AWSRefactoringToolkitFullAccess	2309
Utilisation de cette politique	2309
Détails de la politique	2309
Version de la politique	2310
Document de politique JSON	2310
En savoir plus	2323
AWSRefactoringToolkitSidecarPolicy	2323
Utilisation de cette stratégie	2324
Détails des politiques	2324
Version de la politique	2324
Document de stratégie JSON	2324
En savoir plus	2325
AWSrePostPrivateCloudWatchAccess	2325
Utilisation de cette politique	2325
Détails de la politique	2325
Version de la politique	2326
Document de politique JSON	2326
En savoir plus	2326
AWSRepostSpaceSupportOperationsPolicy	2327
Utilisation de cette politique	2327
Détails de la politique	2327
Version de la politique	2327
Document de politique JSON	2327
En savoir plus	2328
AWSResilienceHubAssessmentExecutionPolicy	2328
Utilisation de cette politique	2328
Détails de la politique	2328
Version de la politique	2329
Document de politique JSON	2329
En savoir plus	2333
AWSResourceAccessManagerFullAccess	2333
Utilisation de cette stratégie	2333
Détails des politiques	2333
Version de la politique	2333
Document de stratégie JSON	2333
En savoir plus	2334

AWSResourceAccessManagerReadOnlyAccess	2334
Utilisation de cette stratégie	2334
Détails des politiques	2334
Version de la politique	2335
Document de stratégie JSON	2335
En savoir plus	2335
AWSResourceAccessManagerResourceShareParticipantAccess	2335
Utilisation de cette stratégie	2336
Détails des politiques	2336
Version de la politique	2336
Document de stratégie JSON	2336
En savoir plus	2337
AWSResourceAccessManagerServiceRolePolicy	2337
Utilisation politique politique	2337
Les politiques	2337
Version de la politique	2337
Document politique JSON	2338
En savoir plus	2338
AWSResourceExplorerFullAccess	2339
Utilisation de cette politique	2339
Détails de la politique	2339
Version de la politique	2339
Document de politique JSON	2339
En savoir plus	2340
AWSResourceExplorerOrganizationsAccess	2340
Utilisation de cette politique	2341
Détails de la politique	2341
Version de la politique	2341
Document de politique JSON	2341
En savoir plus	2343
AWSResourceExplorerReadOnlyAccess	2343
Utilisation de cette politique	2343
Détails de la politique	2343
Version de la politique	2343
Document de politique JSON	2344
En savoir plus	2344

AWSResourceExplorerServiceRolePolicy	2344
Utilisation de cette politique	2345
Détails de la politique	2345
Version de la politique	2345
Document de politique JSON	2345
En savoir plus	2354
AWSResourceGroupsReadOnlyAccess	2354
Utilisation de cette stratégie	2354
Détails des politiques	2355
Version de la politique	2355
Document de stratégie JSON	2355
En savoir plus	2356
AWSRoboMaker_FullAccess	2357
Utilisation de la politique	2357
Détails de politique	2357
Version de la politique	2357
Document de politique JSON	2357
En savoir plus	2358
AWSRoboMakerReadOnlyAccess	2359
Utilisation de cette stratégie	2359
Détails des politiques	2359
Version de la politique	2359
Document de stratégie JSON	2359
En savoir plus	2360
AWSRoboMakerServicePolicy	2360
Utilisation de cette politique	2360
Les détails des politiques	2360
Version de la politique	2360
Document de stratégie JSON	2361
En savoir plus	2362
AWSRoboMakerServiceRolePolicy	2362
Utilisation de cette stratégie	2363
Détails des politiques	2363
Version de la politique	2363
Document de stratégie JSON	2363
En savoir plus	2364

AWSRolesAnywhereServicePolicy	2365
Utilisation de cette politique	2365
Les détails des politiques	2365
Version de la politique	2365
Document de stratégie JSON	2365
En savoir plus	2366
AWSS3OnOutpostsServiceRolePolicy	2366
Utilisation de cette politique	2366
Détails de la politique	2366
Version de la politique	2367
Document de politique JSON	2367
En savoir plus	2369
AWSSavingsPlansFullAccess	2370
Utilisation de cette stratégie	2370
Détails des politiques	2370
Version de la politique	2370
Document de stratégie JSON	2370
En savoir plus	2371
AWSSavingsPlansReadOnlyAccess	2371
Utilisation de cette stratégie	2371
Détails des politiques	2371
Version de la politique	2371
Document de stratégie JSON	2371
En savoir plus	2372
AWSSecurityHubFullAccess	2372
Utilisation de cette politique	2372
Détails de la politique	2372
Version de la politique	2372
Document de politique JSON	2373
En savoir plus	2373
AWSSecurityHubOrganizationsAccess	2374
Utilisation de cette politique	2374
Détails de la politique	2374
Version de la politique	2374
Document de politique JSON	2374
En savoir plus	2376

AWSSecurityHubReadOnlyAccess	2376
Utilisation de cette politique	2376
Détails de la politique	2376
Version de la politique	2376
Document de politique JSON	2376
En savoir plus	2377
AWSSecurityHubServiceRolePolicy	2377
Utilisation de cette politique	2377
Détails de la politique	2377
Version de la politique	2378
Document de politique JSON	2378
En savoir plus	2380
AWSServiceCatalogAdminFullAccess	2380
Utilisation de cette stratégie	2380
Détails des politiques	2380
Version de la politique	2380
Document de stratégie JSON	2381
En savoir plus	2383
AWSServiceCatalogAdminReadOnlyAccess	2383
Utilisation de cette stratégie	2384
Détails des politiques	2384
Version de la politique	2384
Document de stratégie JSON	2384
En savoir plus	2385
AWSServiceCatalogAppRegistryFullAccess	2386
Utilisation de cette politique	2386
Détails de la politique	2386
Version de la politique	2386
Document de politique JSON	2386
En savoir plus	2388
AWSServiceCatalogAppRegistryReadOnlyAccess	2389
Utilisation de cette stratégie	2389
Détails des politiques	2389
Version de la politique	2389
Document de stratégie JSON	2389
En savoir plus	2390

AWSServiceCatalogAppRegistryServiceRolePolicy	2390
Utilisation de cette politique	2390
Les détails des politiques	2390
Version de la politique	2390
Document de stratégie JSON	2391
En savoir plus	2392
AWSServiceCatalogEndUserFullAccess	2392
Utilisation de cette stratégie	2392
Détails des politiques	2392
Version de la politique	2393
Document de stratégie JSON	2393
En savoir plus	2395
AWSServiceCatalogEndUserReadOnlyAccess	2395
Utilisation de cette stratégie	2395
Détails des politiques	2395
Version de la politique	2395
Document de stratégie JSON	2396
En savoir plus	2397
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	2397
les les les les les le	2398
les détails détails les détails	2398
Version de la politique	2398
document de de de de de de	2398
En savoir plus	2399
AWSServiceCatalogSyncServiceRolePolicy	2399
Utilisation	2399
Les politiques	2399
Version de la politique	2399
Document de politique JSON	2400
En savoir plus	2400
AWSServiceRoleForAmazonEKSNodegroup	2401
Utilisation de cette politique	2401
Détails de la politique	2401
Version de la politique	2401
Document de politique JSON	2401
En savoir plus	2405

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy	2406
Utilisation cette politique	2406
Les politiques	2406
Version de la politique	2406
Document de stratégie JSON	2406
En savoir plus	2407
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsSERVICERolePolicy	2407
Utilisation de cette politique	2407
Détails de la politique	2407
Version de la politique	2407
Document de politique JSON	2408
En savoir plus	2408
AWSServiceRoleForCodeGuru-Profiler	2408
Utilisation de cette politique	2408
Les détails des politiques	2408
Version de la politique	2409
Document de stratégie JSON	2409
En savoir plus	2409
AWSServiceRoleForCodeWhispererPolicy	2409
Utilisation de cette politique	2410
Détails de la politique	2410
Version de la politique	2410
Document de politique JSON	2410
En savoir plus	2412
AWSServiceRoleForEC2ScheduledInstances	2412
Utilisation de cette politique	2412
Les détails des politiques	2412
Version de la politique	2413
Document de stratégie JSON	2413
En savoir plus	2414
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	2414
Utilisation de cette politique	2414
Les détails des politiques	2414
Version de la politique	2414
Document de stratégie JSON	2414
En savoir plus	2415

AWSServiceRoleForImageBuilder	2415
Utilisation de cette politique	2415
Détails de la politique	2415
Version de la politique	2416
Document de politique JSON	2416
En savoir plus	2425
AWSServiceRoleForIoTSiteWise	2425
Utilisation de cette politique	2426
Détails de la politique	2426
Version de la politique	2426
Document de politique JSON	2426
En savoir plus	2427
AWSServiceRoleForLogDeliveryPolicy	2428
Utilisation de cette politique	2428
Les détails des politiques	2428
Version de la politique	2428
Document de stratégie JSON	2428
En savoir plus	2429
AWSServiceRoleForMonitronPolicy	2429
Utilisation de cette politique	2429
Les détails des politiques	2429
Version de la politique	2429
Document de politique	2430
En savoir plus	2430
AWSServiceRoleForNeptuneGraphPolicy	2430
Utilisation de cette politique	2431
Détails de la politique	2431
Version de la politique	2431
Document de politique JSON	2431
En savoir plus	2432
AWSServiceRoleForPrivateMarketplaceAdminPolicy	2433
Utilisation de cette politique	2433
Détails de la politique	2433
Version de la politique	2433
Document de politique JSON	2433
En savoir plus	2435

AWSServiceRoleForSMS	2435
Utilisation de cette politique	2435
Les détails des politiques	2435
Version de la politique	2436
Document de stratégie JSON	2436
En savoir plus	2442
AWSServiceRolePolicyForBackupReports	2443
Utilisation de cette politique	2443
Détails des politiques	2443
Version de la politique	2443
Document de politique JSON	2443
En savoir plus	2444
AWSServiceRolePolicyForBackupRestoreTesting	2445
Utilisation de cette politique	2445
Détails de la politique	2445
Version de la politique	2445
Document de politique JSON	2445
En savoir plus	2448
AWSShieldDRTAcessPolicy	2448
Utilisation de cette stratégie	2448
Détails des politiques	2448
Version de la politique	2449
Document de stratégie JSON	2449
En savoir plus	2450
AWSShieldServiceRolePolicy	2450
Utilisation de cette politique	2450
Les détails des politiques	2450
Version de la politique	2450
Document de stratégie JSON	2451
En savoir plus	2451
AWSSSMForSAPServiceLinkedRolePolicy	2451
Utilisation de cette politique	2451
Détails de la politique	2452
Version de la politique	2452
Document de politique JSON	2452
En savoir plus	2458

AWSSSMOpsInsightsServiceRolePolicy	2458
Utilisation de cette politique	2458
Les détails des politiques	2458
Version de la politique	2459
Document de stratégie JSON	2459
En savoir plus	2460
AWSSSODirectoryAdministrator	2460
Utilisation de la stratégie	2460
Détails des stratégies	2460
Version de la politique	2460
Document de stratégie JSON	2460
En savoir plus	2461
AWSSSODirectoryReadOnly	2461
Utilisation de cette stratégie	2461
Détails de stratégie	2461
Version de la politique	2461
Document de stratégie JSON	2462
En savoir plus	2462
AWSSSOMasterAccountAdministrator	2462
Utilisation de cette stratégie	2463
Détails des politiques	2463
Version de la politique	2463
Document de stratégie JSON	2463
En savoir plus	2465
AWSSSOMemberAccountAdministrator	2465
Utilisation de cette stratégie	2465
Détails des politiques	2465
Version de la politique	2465
Document de stratégie JSON	2466
En savoir plus	2467
AWSSSOReadOnly	2467
Utilisation de cette stratégie	2467
Détails des politiques	2467
Version de la politique	2467
Document de stratégie JSON	2468
En savoir plus	2468

AWSSSOServiceRolePolicy	2469
Utilisation de de cette politique	2469
Détails des détails des détails	2469
Version de la politique	2469
Document de de de stratégie JSON	2469
En savoir plus	2473
AWSSStepFunctionsConsoleFullAccess	2473
Utilisation de cette stratégie	2473
Détails des politiques	2473
Version de la politique	2473
Document de stratégie JSON	2474
En savoir plus	2474
AWSSStepFunctionsFullAccess	2475
Utilisation de cette stratégie	2475
Détails des politiques	2475
Version de la politique	2475
Document de stratégie JSON	2475
En savoir plus	2476
AWSSStepFunctionsReadOnlyAccess	2476
Utilisation de cette stratégie	2476
Détails des politiques	2476
Version de la politique	2476
Document de stratégie JSON	2476
En savoir plus	2477
AWSSStorageGatewayFullAccess	2477
Utilisation de cette stratégie	2477
Détails des politiques	2477
Version de la politique	2478
Document de stratégie JSON	2478
En savoir plus	2478
AWSSStorageGatewayReadOnlyAccess	2479
Utilisation de cette stratégie	2479
Détails des politiques	2479
Version de la politique	2479
Document de stratégie JSON	2479
En savoir plus	2480

AWSSStorageGatewayServiceRolePolicy	2480
Utilisation des politique de politique de politique	2480
détails des politique détails des	2480
Version de la politique	2481
Document des stratégie Jpolitique Jpolitique	2481
En savoir plus	2481
AWSSupplyChainFederationAdminAccess	2482
Utilisation de cette politique	2482
Détails de la politique	2482
Version de la politique	2482
Document de politique JSON	2482
En savoir plus	2488
AWSSupportAccess	2488
Utilisation de cette stratégie	2488
Détails des politiques	2488
Version de la politique	2488
Document de stratégie JSON	2489
En savoir plus	2489
AWSSupportAppFullAccess	2489
Utilisation de cette stratégie	2489
Détails des politiques	2489
Version de la politique	2490
Document de stratégie JSON	2490
En savoir plus	2491
AWSSupportAppReadOnlyAccess	2491
Utilisation de cette stratégie	2491
Détails des politiques	2491
Version de la politique	2491
Document de stratégie JSON	2492
En savoir plus	2492
AWSSupportPlansFullAccess	2492
Utilisation de cette stratégie	2492
Détails des politiques	2492
Version de la politique	2493
Document de stratégie JSON	2493
En savoir plus	2493

AWSSupportPlansReadOnlyAccess	2493
Utilisation de cette stratégie	2494
Détails des politiques	2494
Version de la politique	2494
Document de stratégie JSON	2494
En savoir plus	2494
AWSSupportServiceRolePolicy	2495
Utilisation de cette politique	2495
Détails de la politique	2495
Version de la politique	2495
Document de politique JSON	2495
En savoir plus	2569
AWSSystemsManagerAccountDiscoveryServicePolicy	2569
Utilisation de cette politique	2569
Les détails des politiques	2569
Version de la politique	2570
Document de stratégie JSON	2570
En savoir plus	2570
AWSSystemsManagerChangeManagementServicePolicy	2571
Utilisation des politiques politiques politiques politiques	2571
Les détails politiques politiques politiques	2571
Version de la politique	2571
Document de stratégie JSON de stratégie	2571
En savoir plus	2573
AWSSystemsManagerForSAPFullAccess	2573
Utilisation de cette stratégie	2573
Détails des politiques	2573
Version de la politique	2574
Document de stratégie JSON	2574
En savoir plus	2574
AWSSystemsManagerForSAPReadOnlyAccess	2575
Utilisation de cette stratégie	2575
Détails des politiques	2575
Version de la politique	2575
Document de stratégie JSON	2575
En savoir plus	2576

AWSSystemsManagerOpsDataSyncServiceRolePolicy	2576
Utilisation de cette politique	2576
Détails de la politique	2576
Version de la politique	2576
Document de politique JSON	2577
En savoir plus	2580
AWSThinkboxAssetServerPolicy	2580
Utilisation de cette stratégie	2581
Détails des politiques	2581
Version de la politique	2581
Document de stratégie JSON	2581
En savoir plus	2582
AWSThinkboxAWSPortalAdminPolicy	2582
Utilisation de cette politique	2582
Détails de la politique	2582
Version de la politique	2583
Document de politique JSON	2583
En savoir plus	2592
AWSThinkboxAWSPortalGatewayPolicy	2593
Utilisation de cette stratégie	2593
Détails des politiques	2593
Version de la politique	2593
Document de stratégie JSON	2593
En savoir plus	2595
AWSThinkboxAWSPortalWorkerPolicy	2595
Utilisation de cette stratégie	2595
Détails des politiques	2596
Version de la politique	2596
Document de stratégie JSON	2596
En savoir plus	2598
AWSThinkboxDeadlineResourceTrackerAccessPolicy	2598
Utilisation de cette stratégie	2598
Détails des politiques	2598
Version de la politique	2599
Document de stratégie JSON	2599
En savoir plus	2602

AWSThinkboxDeadlineResourceTrackerAdminPolicy	2602
Utilisation de cette stratégie	2602
Détails des politiques	2602
Version de la politique	2602
Document de stratégie JSON	2602
En savoir plus	2608
AWSThinkboxDeadlineSpotEventPluginAdminPolicy	2608
Utilisation de cette stratégie	2608
Détails des politiques	2608
Version de la politique	2609
Document de stratégie JSON	2609
En savoir plus	2612
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	2612
Utilisation de cette stratégie	2612
Détails des politiques	2612
Version de la politique	2612
Document de stratégie JSON	2612
En savoir plus	2614
AWSTransferConsoleFullAccess	2614
Utilisation de cette stratégie	2614
Détails des politiques	2614
Version de la politique	2614
Document de stratégie JSON	2615
En savoir plus	2616
AWSTransferFullAccess	2616
Utilisation de cette stratégie	2616
Détails des politiques	2616
Version de la politique	2616
Document de stratégie JSON	2616
En savoir plus	2617
AWSTransferLoggingAccess	2617
Utilisation de cette stratégie	2618
Détails des politiques	2618
Version de la politique	2618
Document de stratégie JSON	2618
En savoir plus	2619

AWSTransferReadOnlyAccess	2619
Utilisation de cette stratégie	2619
Détails des politiques	2619
Version de la politique	2619
Document de stratégie JSON	2619
En savoir plus	2620
AWSTrustedAdvisorPriorityFullAccess	2620
Utilisation de cette politique	2620
Détails des politiques	2620
Version de la politique	2621
Document de stratégie JSON	2621
En savoir plus	2623
AWSTrustedAdvisorPriorityReadOnlyAccess	2623
Utilisation de cette stratégie	2623
Détails des politiques	2623
Version de la politique	2623
Document de stratégie JSON	2623
En savoir plus	2624
AWSTrustedAdvisorReportingServiceRolePolicy	2625
Utilisation de cette politique	2625
Les détails des politiques	2625
Version de la politique	2625
Document de stratégie JSON	2625
En savoir plus	2626
AWSTrustedAdvisorServiceRolePolicy	2626
Utilisation de cette politique	2626
Détails de la politique	2626
Version de la politique	2627
Document de politique JSON	2627
En savoir plus	2629
AWSUserNotificationsServiceLinkedRolePolicy	2629
Utilisation de cette politique	2630
Détails des politiques	2630
Version de la politique	2630
Document de stratégie JSON	2630
En savoir plus	2631

AWSVendorInsightsAssessorFullAccess	2631
Utilisation de cette stratégie	2631
Détails des politiques	2631
Version de la politique	2632
Document de stratégie JSON	2632
En savoir plus	2633
AWSVendorInsightsAssessorReadOnly	2633
Utilisation de cette stratégie	2633
Détails des politiques	2633
Version de la politique	2634
Document de stratégie JSON	2634
En savoir plus	2634
AWSVendorInsightsVendorFullAccess	2635
Utilisation de cette politique	2635
Détails de la politique	2635
Version de la politique	2635
Document de politique JSON	2635
En savoir plus	2637
AWSVendorInsightsVendorReadOnly	2637
Utilisation de cette stratégie	2637
Détails des politiques	2637
Version de la politique	2638
Document de stratégie JSON	2638
En savoir plus	2639
AWSVpcLatticeServiceRolePolicy	2639
Utilisation des stratégies politique politique politique politique	2639
Les des politique politique politique	2639
Version de la politique	2639
Document politique JSON stratégie JSON	2640
En savoir plus	2640
AWSVPCS2SVpnServiceRolePolicy	2640
Utilisation de cette politique	2640
Détails des politiques	2641
Version de la politique	2641
Document de stratégie JSON	2641
En savoir plus	2641

AWSVPCTransitGatewayServiceRolePolicy	2642
Utilisation utilisation utilisation utilisation utilisation utilisation utilisation	2642
Les détails politiques politiques politiques	2642
Version de la politique	2642
politique Jpolitique Jpolitique Jpolitique	2642
En savoir plus	2643
AWSVPCVerifiedAccessServiceRolePolicy	2643
Utilisation de cette politique	2643
Détails de la politique	2643
Version de la politique	2644
Document de politique JSON	2644
En savoir plus	2645
AWSWAFConsoleFullAccess	2645
Utilisation de cette stratégie	2646
Détails des politiques	2646
Version de la politique	2646
Document de stratégie JSON	2646
En savoir plus	2648
AWSWAFConsoleReadOnlyAccess	2648
Utilisation de cette stratégie	2649
Détails des politiques	2649
Version de la politique	2649
Document de stratégie JSON	2649
En savoir plus	2650
AWSWAFFullAccess	2650
Utilisation de cette stratégie	2650
Détails des politiques	2650
Version de la politique	2651
Document de stratégie JSON	2651
En savoir plus	2652
AWSWAFReadOnlyAccess	2653
Utilisation de cette stratégie	2653
Détails des politiques	2653
Version de la politique	2653
Document de stratégie JSON	2653
En savoir plus	2654

AWSWellArchitectedDiscoveryServiceRolePolicy	2654
Utilisation de cette politique	2654
Les détails des politiques	2654
Version de la politique	2655
Document de politique JSON	2655
En savoir plus	2656
AWSWellArchitectedOrganizationsServiceRolePolicy	2657
Utilisation de cette politique	2657
Les détails des politiques	2657
Version de la politique	2657
Document de stratégie JSON	2657
En savoir plus	2658
AWSWickrFullAccess	2658
Utilisation de cette stratégie	2658
Détails des politiques	2658
Version de la politique	2658
Document de stratégie JSON	2659
En savoir plus	2659
AWSXrayCrossAccountSharingConfiguration	2659
Utilisation de cette stratégie	2659
Détails des politiques	2659
Version de la politique	2660
Document de stratégie JSON	2660
En savoir plus	2661
AWSXRayDaemonWriteAccess	2661
Utilisation de cette politique	2661
Détails de la politique	2661
Version de la politique	2661
Document de politique JSON	2662
En savoir plus	2662
AWSXrayFullAccess	2662
Utilisation de cette stratégie	2662
Détails des politiques	2663
Version de la politique	2663
Document de stratégie JSON	2663
En savoir plus	2663

AWSXrayReadOnlyAccess	2664
Utilisation de cette politique	2664
Détails de la politique	2664
Version de la politique	2664
Document de politique JSON	2664
En savoir plus	2665
AWSXrayWriteOnlyAccess	2665
Utilisation de cette stratégie	2665
Détails des politiques	2665
Version de la politique	2666
Document de stratégie JSON	2666
En savoir plus	2666
AWSZonalAutoshiftPracticeRunSLRPolicy	2667
Utilisation de cette politique	2667
Détails de la politique	2667
Version de la politique	2667
Document de politique JSON	2667
En savoir plus	2668
BatchServiceRolePolicy	2668
Utilisation de cette politique	2668
Détails de la politique	2668
Version de la politique	2669
Document de politique JSON	2669
En savoir plus	2675
Billing	2675
Utilisation de cette politique	2675
Détails de la politique	2675
Version de la politique	2675
Document de politique JSON	2676
En savoir plus	2678
CertificateManagerServiceRolePolicy	2678
Utilisation de cette politique politique politique	2679
Les détails des politiques politiques	2679
Version de la politique	2679
Document de stratégie JAM JAM	2679
En savoir plus	2680

ClientVPNServiceConnectionsRolePolicy	2680
Utilisation de de de de de des	2680
Les des des des des	2680
Version de la politique	2680
Document de de de de de des	2680
En savoir plus	2681
ClientVPNServiceRolePolicy	2681
Utilisation de stratégie	2681
Détails de politique	2681
Version de la politique	2681
Document de stratégie JSON	2682
En savoir plus	2682
CloudFormationStackSetsOrgAdminServiceRolePolicy	2683
Utilisation à cette politique	2683
Les détails de la politique	2683
Version de la politique	2683
Document de stratégie JSON	2683
En savoir plus	2684
CloudFormationStackSetsOrgMemberServiceRolePolicy	2684
Utilisation de cette politique	2684
Les détails des politiques	2684
Version de la politique	2684
Document de stratégie JSON	2685
En savoir plus	2685
CloudFrontFullAccess	2686
Utilisation de cette politique	2686
Détails de la politique	2686
Version de la politique	2686
Document de politique JSON	2686
En savoir plus	2687
CloudFrontReadOnlyAccess	2688
Utilisation de cette politique	2688
Détails de la politique	2688
Version de la politique	2688
Document de politique JSON	2688
En savoir plus	2689

CloudHSMSERVICERolePolicy	2689
Utilisation politiques Utilisation politiques	2689
détails détails politiques	2689
Version de la politique	2690
Document politiques JSON	2690
En savoir plus	2690
CloudSearchFullAccess	2690
Utilisation de cette stratégie	2691
Détails des politiques	2691
Version de la politique	2691
Document de stratégie JSON	2691
En savoir plus	2691
CloudSearchReadOnlyAccess	2692
Utilisation de cette stratégie	2692
Détails des politiques	2692
Version de la politique	2692
Document de stratégie JSON	2692
En savoir plus	2693
CloudTrailServiceRolePolicy	2693
Utilisation de cette politique	2693
Détails de la politique	2693
Version de la politique	2693
Document de politique JSON	2694
En savoir plus	2695
CloudWatch-CrossAccountAccess	2695
Utilisation de cette politique	2695
Les détails des politiques	2696
Version de la politique	2696
Document de stratégie JSON	2696
En savoir plus	2696
CloudWatchActionsEC2Access	2697
Utilisation de cette stratégie	2697
Détails des politiques	2697
Version de la politique	2697
Document de stratégie JSON	2697
En savoir plus	2698

CloudWatchAgentAdminPolicy	2698
Utilisation de cette politique	2698
Détails de la politique	2698
Version de la politique	2698
Document de politique JSON	2699
En savoir plus	2699
CloudWatchAgentServerPolicy	2700
Utilisation de cette politique	2700
Détails de la politique	2700
Version de la politique	2700
Document de politique JSON	2700
En savoir plus	2701
CloudWatchApplicationInsightsFullAccess	2701
Utilisation de cette stratégie	2701
Détails des politiques	2702
Version de la politique	2702
Document de stratégie JSON	2702
En savoir plus	2703
CloudWatchApplicationInsightsReadOnlyAccess	2704
Utilisation de cette stratégie	2704
Détails des politiques	2704
Version de la politique	2704
Document de stratégie JSON	2704
En savoir plus	2705
CloudwatchApplicationInsightsServiceLinkedRolePolicy	2705
Utilisation de cette politique	2705
Les détails des politiques	2705
Version de la politique	2705
Document de stratégie JSON	2706
En savoir plus	2715
CloudWatchApplicationSignalsServiceRolePolicy	2715
Utilisation de cette politique	2716
Détails de la politique	2716
Version de la politique	2716
Document de politique JSON	2716
En savoir plus	2718

CloudWatchAutomaticDashboardsAccess	2718
Utilisation de cette stratégie	2718
Détails des politiques	2718
Version de la politique	2718
Document de stratégie JSON	2719
En savoir plus	2720
CloudWatchCrossAccountSharingConfiguration	2720
Utilisation de cette stratégie	2720
Détails des politiques	2720
Version de la politique	2721
Document de stratégie JSON	2721
En savoir plus	2722
CloudWatchEventsBuiltInTargetExecutionAccess	2722
Utilisation de cette stratégie	2722
Détails des politiques	2722
Version de la politique	2722
Document de stratégie JSON	2723
En savoir plus	2723
CloudWatchEventsFullAccess	2723
Utilisation de cette stratégie	2723
Détails des politiques	2724
Version de la politique	2724
Document de stratégie JSON	2724
En savoir plus	2726
CloudWatchEventsInvocationAccess	2726
Utilisation de cette stratégie	2726
Détails des politiques	2726
Version de la politique	2727
Document de stratégie JSON	2727
En savoir plus	2727
CloudWatchEventsReadOnlyAccess	2727
Utilisation de cette stratégie	2728
Détails des politiques	2728
Version de la politique	2728
Document de stratégie JSON	2728
En savoir plus	2729

CloudWatchEventsServiceRolePolicy	2730
Utilisation de cette politique politique politique	2730
Utilisation des politiques politiques politiques	2730
Version de la politique	2730
Document de stratégie de politique de politique	2730
En savoir plus	2731
CloudWatchFullAccess	2731
Utilisation de cette stratégie	2731
Détails des politiques	2731
Version de la politique	2732
Document de stratégie JSON	2732
En savoir plus	2733
CloudWatchFullAccessV2	2733
Utilisation de cette politique	2733
Détails de la politique	2733
Version de la politique	2733
Document de politique JSON	2734
En savoir plus	2735
CloudWatchInternetMonitorServiceRolePolicy	2735
Utilisation de cette politique	2735
Détails de la politique	2736
Version de la politique	2736
Document de politique JSON	2736
En savoir plus	2737
CloudWatchLambdaInsightsExecutionRolePolicy	2737
Utilisation de cette stratégie	2737
Détails des politiques	2737
Version de la politique	2738
Document de stratégie JSON	2738
En savoir plus	2738
CloudWatchLogsCrossAccountSharingConfiguration	2739
Utilisation de cette stratégie	2739
Détails des politiques	2739
Version de la politique	2739
Document de stratégie JSON	2739
En savoir plus	2740

CloudWatchLogsFullAccess	2740
Utilisation de cette politique	2740
Détails de la politique	2741
Version de la politique	2741
Document de politique JSON	2741
En savoir plus	2741
CloudWatchLogsReadOnlyAccess	2742
Utilisation de cette politique	2742
Détails de la politique	2742
Version de la politique	2742
Document de politique JSON	2742
En savoir plus	2743
CloudWatchNetworkMonitorServiceRolePolicy	2743
Utilisation de cette politique	2743
Détails de la politique	2743
Version de la politique	2744
Document de politique JSON	2744
En savoir plus	2745
CloudWatchReadOnlyAccess	2745
Utilisation de cette politique	2745
Détails de la politique	2745
Version de la politique	2746
Document de politique JSON	2746
En savoir plus	2747
CloudWatchSyntheticsFullAccess	2747
Utilisation de cette stratégie	2747
Détails de la stratégie	2747
Version de la politique	2748
Document de stratégie JSON	2748
En savoir plus	2752
CloudWatchSyntheticsReadOnlyAccess	2753
Utilisation de cette stratégie	2753
Détails de la stratégie	2753
Version de la politique	2753
Document de stratégie JSON	2753
En savoir plus	2754

ComprehendDataAccessRolePolicy	2754
Utilisation de cette stratégie	2754
Détails des politiques	2754
Version de la politique	2754
Document de stratégie JSON	2754
En savoir plus	2755
ComprehendFullAccess	2755
Utilisation de cette stratégie	2755
Détails des politiques	2755
Version de la politique	2756
Document de stratégie JSON	2756
En savoir plus	2756
ComprehendMedicalFullAccess	2756
Utilisation de cette stratégie	2757
Détails des politiques	2757
Version de la politique	2757
Document de stratégie JSON	2757
En savoir plus	2757
ComprehendReadOnly	2758
Utilisation de cette stratégie	2758
Détails des politiques	2758
Version de la politique	2758
Document de stratégie JSON	2758
En savoir plus	2759
ComputeOptimizerReadOnlyAccess	2760
Utilisation de cette politique	2760
Détails de la politique	2760
Version de la politique	2760
Document de politique JSON	2760
En savoir plus	2761
ComputeOptimizerServiceRolePolicy	2762
Utilisation de cette politique	2762
Les détails des politiques	2762
Version de la politique	2762
Document de stratégie JSON Document de	2762
En savoir plus	2764

ConfigConformsServiceRolePolicy	2764
Utilisation de cette politique de cette politique	2764
Les détails des politiques politiques	2764
Version de la politique	2764
Document de stratégie JSON	2764
En savoir plus	2767
CostOptimizationHubAdminAccess	2767
Utilisation de cette politique	2767
Détails de la politique	2768
Version de la politique	2768
Document de politique JSON	2768
En savoir plus	2769
CostOptimizationHubReadOnlyAccess	2769
Utilisation de cette politique	2770
Détails de la politique	2770
Version de la politique	2770
Document de politique JSON	2770
En savoir plus	2771
CostOptimizationHubServiceRolePolicy	2771
Utilisation de cette politique	2771
Détails de la politique	2771
Version de la politique	2771
Document de politique JSON	2771
En savoir plus	2772
CustomerProfilesServiceLinkedRolePolicy	2772
Utilisation de de de de de de	2773
détails les détails les détails	2773
Version de la politique	2773
Document de	2773
En savoir plus	2774
DatabaseAdministrator	2774
Utilisation de cette stratégie	2774
Détails des politiques	2774
Version de la politique	2774
Document de stratégie JSON	2775
En savoir plus	2777

DataScientist	2777
Utilisation de cette stratégie	2777
Détails des politiques	2777
Version de la politique	2778
Document de stratégie JSON	2778
En savoir plus	2781
DAXServiceRolePolicy	2782
Utilisation de de de cette politique	2782
des des politiques	2782
Version de la politique	2782
de stratégie de politique de JSON	2782
En savoir plus	2783
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	2783
Utilisation de cette politique	2783
Les détails des politiques	2783
Version de la politique	2784
Document JSON	2784
En savoir plus	2784
DynamoDBKinesisReplicationServiceRolePolicy	2784
Utilisation de cette politique	2785
Détails des politiques	2785
Version de la politique	2785
Document de politique JSON	2785
En savoir plus	2786
DynamoDBReplicationServiceRolePolicy	2786
Utilisation de cette politique	2786
Détails de la politique	2786
Version de la politique	2786
Document de politique JSON	2787
En savoir plus	2788
EC2FastLaunchServiceRolePolicy	2788
Utilisation	2788
Policy details	2788
Version de la politique	2788
Document de stratégie	2789
En savoir plus	2792

EC2FleetTimeShiftableServiceRolePolicy	2793
Utilisation des stratégies	2793
Les détails des	2793
Version de la politique	2793
Document de	2793
En savoir plus	2795
Ec2ImageBuilderCrossAccountDistributionAccess	2795
Utilisation de cette stratégie	2795
Détails des politiques	2795
Version de la politique	2795
Document de stratégie JSON	2795
En savoir plus	2796
EC2ImageBuilderLifecycleExecutionPolicy	2796
Utilisation de cette politique	2796
Détails de la politique	2797
Version de la politique	2797
Document de politique JSON	2797
En savoir plus	2799
EC2InstanceConnect	2799
Utilisation de cette stratégie	2799
Détails des politiques	2799
Version de la politique	2800
Document de stratégie JSON	2800
En savoir plus	2800
Ec2InstanceConnectEndpoint	2800
Utilisation des stratégies	2801
Les détails des politiques	2801
Version de la politique	2801
Document de stratégie JSON	2801
En savoir plus	2803
EC2InstanceProfileForImageBuilder	2803
Utilisation de cette stratégie	2803
Détails des politiques	2803
Version de la politique	2804
Document de stratégie JSON	2804
En savoir plus	2805

EC2InstanceProfileForImageBuilderECRContainerBuilds	2805
Utilisation de cette stratégie	2805
Détails des politiques	2805
Version de la politique	2806
Document de stratégie JSON	2806
En savoir plus	2807
ECRReplicationServiceRolePolicy	2807
Utilisation de cette politique	2808
Les détails des politiques	2808
Version de la politique	2808
Document de stratégie JSON JSON	2808
En savoir plus	2809
ElastiCacheServiceRolePolicy	2809
Utilisation de cette politique	2809
Détails de la politique	2809
Version de la politique	2809
Document de politique JSON	2809
En savoir plus	2811
ElasticLoadBalancingFullAccess	2812
Utilisation de cette stratégie	2812
Détails des politiques	2812
Version de la politique	2812
Document de stratégie JSON	2812
En savoir plus	2814
ElasticLoadBalancingReadOnly	2814
Utilisation de cette politique	2814
Détails de la politique	2814
Version de la politique	2814
Document de politique JSON	2814
En savoir plus	2815
ElementalActivationsDownloadSoftwareAccess	2816
Utilisation de cette stratégie	2816
Détails des politiques	2816
Version de la politique	2816
Document de stratégie JSON	2816
En savoir plus	2817

ElementalActivationsFullAccess	2817
Utilisation de cette stratégie	2817
Détails des politiques	2817
Version de la politique	2817
Document de stratégie JSON	2818
En savoir plus	2818
ElementalActivationsGenerateLicenses	2818
Utilisation de cette stratégie	2818
Détails des politiques	2818
Version de la politique	2819
Document de stratégie JSON	2819
En savoir plus	2819
ElementalActivationsReadOnlyAccess	2819
Utilisation de cette stratégie	2820
Détails des politiques	2820
Version de la politique	2820
Document de stratégie JSON	2820
En savoir plus	2820
ElementalAppliancesSoftwareFullAccess	2821
Utilisation de cette stratégie	2821
Détails des politiques	2821
Version de la politique	2821
Document de stratégie JSON	2821
En savoir plus	2822
ElementalAppliancesSoftwareReadOnlyAccess	2822
Utilisation de cette stratégie	2822
Détails des politiques	2822
Version de la politique	2822
Document de stratégie JSON	2823
En savoir plus	2823
ElementalSupportCenterFullAccess	2823
Utilisation de cette stratégie	2823
Détails des politiques	2824
Version de la politique	2824
Document de stratégie JSON	2824
En savoir plus	2824

EMRDescribeClusterPolicyForEMRWAL	2825
Utilisation de cette politique	2825
Détails de la politique	2825
Version de la politique	2825
Document de politique JSON	2825
En savoir plus	2826
FMSServiceRolePolicy	2826
Utilisation de cette politique	2826
Les détails des politiques	2826
Version de la politique	2826
Document de politique JSON	2827
En savoir plus	2841
FSxDeleteServiceLinkedRoleAccess	2841
Utilisation de cette politique	2841
Les détails des politiques	2841
Version de la politique	2841
Document de stratégie JSON	2841
En savoir plus	2842
GameLiftGameServerGroupPolicy	2842
Utilisation de cette stratégie	2842
Détails des politiques	2842
Version de la politique	2842
Document de stratégie JSON	2843
En savoir plus	2844
GlobalAcceleratorFullAccess	2844
Utilisation de cette stratégie	2845
Détails des politiques	2845
Version de la politique	2845
Document de stratégie JSON	2845
En savoir plus	2846
GlobalAcceleratorReadOnlyAccess	2846
Utilisation de cette stratégie	2846
Détails des politiques	2847
Version de la politique	2847
Document de stratégie JSON	2847
En savoir plus	2847

GreengrassOTAUpdateArtifactAccess	2848
Utilisation de cette stratégie	2848
Détails des politiques	2848
Version de la politique	2848
Document de stratégie JSON	2848
En savoir plus	2849
GroundTruthSyntheticConsoleFullAccess	2849
Utilisation de cette stratégie	2849
Détails des politiques	2849
Version de la politique	2849
Document de stratégie JSON	2850
En savoir plus	2850
GroundTruthSyntheticConsoleReadOnlyAccess	2850
Utilisation de cette stratégie	2850
Détails des politiques	2850
Version de la politique	2851
Document de stratégie JSON	2851
En savoir plus	2851
Health_OrganizationsServiceRolePolicy	2852
Utilisation de cette politique	2852
Détails de la politique	2852
Version de la politique	2852
Document de politique JSON	2852
En savoir plus	2853
IAMAccessAdvisorReadOnly	2853
Utilisation de cette stratégie	2853
Détails des politiques	2853
Version de la politique	2853
Document de stratégie JSON	2854
En savoir plus	2854
IAMAccessAnalyzerFullAccess	2855
Utilisation de cette stratégie	2855
Détails des politiques	2855
Version de la politique	2855
Document de stratégie JSON	2855
En savoir plus	2856

IAMAccessAnalyzerReadOnlyAccess	2857
Utilisation de cette politique	2857
Détails de la politique	2857
Version de la politique	2857
Document de politique JSON	2857
En savoir plus	2858
IAMFullAccess	2858
Utilisation de cette stratégie	2858
Détails des politiques	2858
Version de la politique	2858
Document de stratégie JSON	2859
En savoir plus	2859
IAMReadOnlyAccess	2859
Utilisation de cette stratégie	2859
Détails des politiques	2860
Version de la politique	2860
Document de stratégie JSON	2860
En savoir plus	2860
IAMSelfManageServiceSpecificCredentials	2861
Utilisation de cette stratégie	2861
Détails des politiques	2861
Version de la politique	2861
Document de stratégie JSON	2861
En savoir plus	2862
IAMUserChangePassword	2862
Utilisation de cette stratégie	2862
Détails des politiques	2862
Version de la politique	2862
Document de stratégie JSON	2863
En savoir plus	2863
IAMUserSSHKeys	2863
Utilisation de cette stratégie	2864
Détails des politiques	2864
Version de la politique	2864
Document de stratégie JSON	2864
En savoir plus	2865

IVSFullAccess	2865
Utilisation de cette politique	2865
Détails de la politique	2865
Version de la politique	2865
Document de politique JSON	2865
En savoir plus	2866
IVSReadOnlyAccess	2866
Utilisation de cette politique	2866
Détails de la politique	2866
Version de la politique	2866
Document de politique JSON	2867
En savoir plus	2868
IVSRecordToS3	2868
des politique	2868
Policy details	2868
Version de la politique	2868
document de politique	2869
En savoir plus	2869
KafkaConnectServiceRolePolicy	2869
Les politiques de cette politique de politique	2869
les politiques politiques politiques politiques	2869
Version de la politique	2870
JSON des politiques JSON des	2870
En savoir plus	2871
KafkaServiceRolePolicy	2871
Utilisation de cette politique	2872
Les détails des politiques	2872
Version de la politique	2872
Document de politique JSON	2872
En savoir plus	2874
KeyspacesReplicationServiceRolePolicy	2874
Utilisation de cette politique	2874
Détails politiques	2874
Version de la politique	2874
Document de stratégie son document de politique	2874
En savoir plus	2875

LakeFormationDataAccessServiceRolePolicy	2875
Utilisation de cette politique	2875
Détails de la politique	2875
Version de la politique	2875
Document de politique JSON	2876
En savoir plus	2876
LexBotPolicy	2876
Utilisation de cette politique	2876
Les détails des politiques	2876
Version de la politique	2877
Document de politique JSON	2877
En savoir plus	2878
LexChannelPolicy	2878
Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation	2878
Les détails des politiques	2878
Version de la politique	2878
Document de stratégie JSON	2878
En savoir plus	2879
LightsailExportAccess	2879
Utilisation de cette politique	2879
Les détails des politiques	2879
Version de la politique	2879
Document de stratégie JSON	2880
En savoir plus	2880
MediaConnectGatewayInstanceRolePolicy	2881
Utilisation de cette stratégie	2881
Détails des politiques	2881
Version de la politique	2881
Document de stratégie JSON	2881
En savoir plus	2882
MediaPackageServiceRolePolicy	2882
Utilisation de cette politique	2882
Les détails des politiques	2882
Version de la politique	2882
Document de politique JSON	2883
En savoir plus	2883

MemoryDBServiceRolePolicy	2883
Utilisation de cette politique	2883
Détails des politiques	2884
Version de la politique	2884
Document de stratégie JSON	2884
En savoir plus	2886
MigrationHubDMSAccessServiceRolePolicy	2886
Utilisation de cette politique	2886
Détails des politiques	2886
Version de la politique	2886
Document de stratégie JSON	2887
En savoir plus	2888
MigrationHubServiceRolePolicy	2888
Utilisation utilisation utilisation utilisation utilisation de politiques	2888
détails des politiques en politiques	2888
Version de la politique	2888
document de stratégie JSON SON SON	2888
En savoir plus	2890
MigrationHubSMSAccessServiceRolePolicy	2890
Utilisation de cette politique	2890
Les détails des politiques	2890
Version de la politique	2890
Document de stratégie JSON	2891
En savoir plus	2892
MonitronServiceRolePolicy	2892
Utilisation de cette politique	2892
Les politiques	2892
Version de la politique	2892
Document de politique JSON	2892
En savoir plus	2893
NeptuneConsoleFullAccess	2893
Utilisation de cette politique	2893
Détails de la politique	2893
Version de la politique	2894
Document de politique JSON	2894
En savoir plus	2899

NeptuneFullAccess	2899
Utilisation de cette politique	2900
Détails de la politique	2900
Version de la politique	2900
Document de politique JSON	2900
En savoir plus	2904
NeptuneGraphReadOnlyAccess	2904
Utilisation de cette politique	2904
Détails de la politique	2904
Version de la politique	2905
Document de politique JSON	2905
En savoir plus	2906
NeptuneReadOnlyAccess	2907
Utilisation de cette politique	2907
Détails de la politique	2907
Version de la politique	2907
Document de politique JSON	2907
En savoir plus	2909
NetworkAdministrator	2910
Utilisation de cette stratégie	2910
Détails des politiques	2910
Version de la politique	2910
Document de stratégie JSON	2910
En savoir plus	2917
OAMFullAccess	2917
Utilisation de cette stratégie	2917
Détails des politiques	2917
Version de la politique	2917
Document de stratégie JSON	2918
En savoir plus	2918
OAMReadOnlyAccess	2918
Utilisation de cette stratégie	2918
Détails des politiques	2918
Version de la politique	2919
Document de stratégie JSON	2919
En savoir plus	2919

PartnerCentralAccountManagementUserRoleAssociation	2919
Utilisation de cette politique	2920
Détails de la politique	2920
Version de la politique	2920
Document de politique JSON	2920
En savoir plus	2921
PowerUserAccess	2921
Utilisation de cette politique	2921
Détails de la politique	2921
Version de la politique	2921
Document de politique JSON	2922
En savoir plus	2922
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	2923
Utilisation de cette stratégie	2923
Détails des politiques	2923
Version de la politique	2923
Document de stratégie JSON	2923
En savoir plus	2924
RDSCloudHsmAuthorizationRole	2924
Utilisation de cette stratégie	2924
Détails des politiques	2924
Version de la politique	2925
Document de stratégie JSON	2925
En savoir plus	2925
ReadOnlyAccess	2926
Utilisation de cette politique	2926
Détails de la politique	2926
Version de la politique	2926
Document de politique JSON	2926
En savoir plus	2972
ResourceGroupsandTagEditorFullAccess	2973
Utilisation de cette politique	2973
Détails de la politique	2973
Version de la politique	2973
Document de politique JSON	2973
En savoir plus	2974

ResourceGroupsandTagEditorReadOnlyAccess	2974
Utilisation de cette politique	2974
Détails de la politique	2974
Version de la politique	2975
Document de politique JSON	2975
En savoir plus	2975
ResourceGroupsServiceRolePolicy	2976
Utilisation de cette politique	2976
Les détails des politiques	2976
Version de la politique	2976
Document de stratégie JSON	2976
En savoir plus	2977
ROSAAmazonEBSCSIDriverOperatorPolicy	2977
Utilisation de cette stratégie	2977
Détails des politiques	2977
Version de la politique	2977
Document de stratégie JSON	2978
En savoir plus	2981
ROSACloudNetworkConfigOperatorPolicy	2981
Utilisation de cette stratégie	2981
Détails des politiques	2981
Version de la politique	2981
Document de stratégie JSON	2982
En savoir plus	2982
ROSAControlPlaneOperatorPolicy	2983
Utilisation de cette politique	2983
Détails de la politique	2983
Version de la politique	2983
Document de politique JSON	2983
En savoir plus	2988
ROSAImageRegistryOperatorPolicy	2988
Utilisation de cette politique	2988
Détails de la politique	2988
Version de la politique	2988
Document de politique JSON	2989
En savoir plus	2990

ROSAIngressOperatorPolicy	2990
Utilisation de cette stratégie	2990
Détails des politiques	2990
Version de la politique	2991
Document de stratégie JSON	2991
En savoir plus	2992
ROSAInstallerPolicy	2992
Utilisation de cette politique	2992
Détails de la politique	2992
Version de la politique	2992
Document de politique JSON	2992
En savoir plus	3000
ROSAKMSProviderPolicy	3000
Utilisation de cette stratégie	3000
Détails des politiques	3000
Version de la politique	3000
Document de stratégie JSON	3000
En savoir plus	3001
ROSAKubeControllerPolicy	3001
Utilisation de cette politique	3001
Détails de la politique	3001
Version de la politique	3002
Document de politique JSON	3002
En savoir plus	3006
ROSAManageSubscription	3006
Utilisation de cette politique	3007
Détails de la politique	3007
Version de la politique	3007
Document de politique JSON	3007
En savoir plus	3008
ROSANodePoolManagementPolicy	3008
Utilisation de cette stratégie	3008
Détails des politiques	3008
Version de la politique	3009
Document de stratégie JSON	3009
En savoir plus	3014

ROSASRESupportPolicy	3015
Utilisation de cette politique	3015
Détails de la politique	3015
Version de la politique	3015
Document de politique JSON	3015
En savoir plus	3020
ROSAWorkerInstancePolicy	3020
Utilisation de cette stratégie	3020
Détails des politiques	3020
Version de la politique	3021
Document de stratégie JSON	3021
En savoir plus	3021
Route53RecoveryReadinessServiceRolePolicy	3022
Utilisation de cette politique	3022
Les détails des politiques	3022
Version de la politique	3022
Document de stratégie JSON	3022
En savoir plus	3026
Route53ResolverServiceRolePolicy	3026
des	3026
Les détails des politiques	3026
Version de la politique	3026
JSON policy document	3027
En savoir plus	3027
S3StorageLensServiceRolePolicy	3027
Utilisation des des des de cette politique	3027
Détails des détails des détails	3027
Version de la politique	3028
Document des d'un document de politique	3028
En savoir plus	3028
SecretsManagerReadWrite	3029
Utilisation de cette politique	3029
Détails de la politique	3029
Version de la politique	3029
Document de politique JSON	3029
En savoir plus	3031

SecurityAudit	3031
Utilisation de cette politique	3031
Détails de la politique	3031
Version de la politique	3031
Document de politique JSON	3032
En savoir plus	3047
SecurityLakeServiceLinkedRole	3047
Utilisation de cette politique	3048
Détails de la politique	3048
Version de la politique	3048
Document de politique JSON	3048
En savoir plus	3051
ServerMigration_ServiceRole	3051
Utilisation de cette stratégie	3051
Détails des politiques	3051
Version de la politique	3051
Document de stratégie JSON	3051
En savoir plus	3056
ServerMigrationConnector	3056
Utilisation de cette stratégie	3057
Détails des politiques	3057
Version de la politique	3057
Document de stratégie JSON	3057
En savoir plus	3059
ServerMigrationServiceConsoleFullAccess	3059
Utilisation de cette stratégie	3059
Détails des politiques	3059
Version de la politique	3059
Document de stratégie JSON	3059
En savoir plus	3061
ServerMigrationServiceLaunchRole	3061
Utilisation de cette stratégie	3061
Détails des politiques	3061
Version de la politique	3062
Document de stratégie JSON	3062
En savoir plus	3065

ServerMigrationServiceRoleForInstanceValidation	3065
Utilisation de cette stratégie	3065
Détails des politiques	3065
Version de la politique	3065
Document de stratégie JSON	3065
En savoir plus	3066
ServiceQuotasFullAccess	3066
Utilisation de cette stratégie	3066
Détails des politiques	3066
Version de la politique	3067
Document de stratégie JSON	3067
En savoir plus	3068
ServiceQuotasReadOnlyAccess	3069
Utilisation de cette stratégie	3069
Détails des politiques	3069
Version de la politique	3069
Document de stratégie JSON	3069
En savoir plus	3070
ServiceQuotasServiceRolePolicy	3070
Utilisation de cette politique	3071
Les détails des politiques	3071
Version de la politique	3071
Document de stratégie JSON	3071
En savoir plus	3072
SimpleWorkflowFullAccess	3072
Utilisation de cette stratégie	3072
Détails des politiques	3072
Version de la politique	3072
Document de stratégie JSON	3072
En savoir plus	3073
SupportUser	3073
Utilisation de cette politique	3073
Détails de la politique	3073
Version de la politique	3073
Document de politique JSON	3074
En savoir plus	3079

SystemAdministrator	3079
Utilisation de cette stratégie	3079
Détails des politiques	3079
Version de la politique	3079
Document de stratégie JSON	3079
En savoir plus	3085
TranslateFullAccess	3086
Utilisation de cette stratégie	3086
Détails des politiques	3086
Version de la politique	3086
Document de stratégie JSON	3086
En savoir plus	3087
TranslateReadOnly	3087
Utilisation de cette stratégie	3087
Détails des politiques	3087
Version de la politique	3087
Document de stratégie JSON	3088
En savoir plus	3088
ViewOnlyAccess	3088
Utilisation de cette stratégie	3088
Détails des politiques	3089
Version de la politique	3089
Document de stratégie JSON	3089
En savoir plus	3095
VMImportExportRoleForAWSConnector	3095
Utilisation de cette stratégie	3095
Détails des politiques	3095
Version de la politique	3096
Document de stratégie JSON	3096
En savoir plus	3096
VPCLatticeFullAccess	3097
Utilisation de cette stratégie	3097
Détails des politiques	3097
Version de la politique	3097
Document de stratégie JSON	3097
En savoir plus	3099

VPCLatticeReadOnlyAccess	3099
Utilisation de cette stratégie	3100
Détails des politiques	3100
Version de la politique	3100
Document de stratégie JSON	3100
En savoir plus	3101
VPCLatticeServicesInvokeAccess	3101
Utilisation de cette stratégie	3101
Détails des politiques	3101
Version de la politique	3102
Document de stratégie JSON	3102
En savoir plus	3102
WAFLoggingServiceRolePolicy	3102
Utilisation de cette politique en utilisation de	3102
Les détails des politiques,	3103
Version de la politique	3103
Document de stratégie JSON politique J	3103
En savoir plus	3103
WAFRegionalLoggingServiceRolePolicy	3104
Utilisation de politique	3104
Détails des politique	3104
Version de la politique	3104
Document de politique JSON	3104
En savoir plus	3105
WAFV2LoggingServiceRolePolicy	3105
Utilisation de cette politique	3105
Les détails des politiques	3105
Version de la politique	3105
Document de stratégie JSON	3106
En savoir plus	3106
WellArchitectedConsoleFullAccess	3106
Utilisation de cette stratégie	3106
Détails des politiques	3107
Version de la politique	3107
Document de stratégie JSON	3107
En savoir plus	3107

WellArchitectedConsoleReadOnlyAccess	3108
Utilisation de cette politique	3108
Détails de la politique	3108
Version de la politique	3108
Document de politique JSON	3108
En savoir plus	3109
WorkLinkServiceRolePolicy	3109
Utilisation de cette stratégie	3109
Détails des stratégies	3109
Version de la politique	3109
Document de stratégie JSON	3109
En savoir plus	3110
.....	mmmcxi

Que sont les politiques AWS gérées ?

Une politique AWS gérée est une politique autonome créée et administrée par AWS. Les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants. Ils vous permettent de commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles plus facilement que si vous deviez rédiger vous-même les politiques.

Gardez à l'esprit que les AWS politiques gérées peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles peuvent être utilisées par tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont spécifiques à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

Comprendre les pages de référence des politiques

Chaque page de référence des politiques inclut les informations suivantes :

- Utilisation de cette politique : si vous pouvez associer la politique aux utilisateurs, aux groupes et aux rôles
- Détails de la politique
 - Type : type de politique AWS gérée
 - `AWS managed policy`— Une politique AWS gérée standard
 - `Job function policy`— Politique alignée sur les fonctions professionnelles courantes de l'industrie
 - `Service-linked role policy`— Politique attachée à un rôle lié à un service qui permet à un service d'effectuer des actions en votre nom, telles que [the section called "AmazonRDSPreviewServiceRolePolicy"](#)
 - `Service role policy`— Politique conçue pour fonctionner avec les rôles de service, tels que [the section called "AWSControlTowerServiceRolePolicy"](#)

- Heure de création : date à laquelle la politique a été créée pour la première fois
- Heure de modification : date à laquelle cette version de la politique a été modifiée
- ARN — Le nom de ressource Amazon de la politique
- Version de la politique : version des autorisations accordées par la politique
- Document de politique JSON — La politique JSON
- En savoir plus — Liens vers la documentation relative aux politiques AWS gérées

Politiques gérées par AWS obsolètes

AWS met régulièrement à jour les politiques AWS gérées. Dans la plupart des cas, nous ajoutons des autorisations à une politique. Cela se produit lorsque nous lançons un nouveau service ou une nouvelle fonctionnalité. Pour améliorer la sécurité des politiques AWS gérées, nous réduisons parfois le champ d'application des politiques. Lorsque nous supprimons des autorisations d'une politique, nous la définissons comme obsolète et nous en rendons une nouvelle disponible. Lorsque vous AWS dépréciez un service ou une fonctionnalité, nous désapprouvons également la politique AWS gérée pour cette fonctionnalité.

Si vous recevez une notification par e-mail indiquant qu'une politique que vous utilisez est obsolète, nous vous recommandons d'agir immédiatement. Identifiez le changement apporté à la politique et mettez à jour vos flux de travail. S'il AWS fournit une politique de remplacement, prévoyez de l'associer à toutes les identités concernées (utilisateurs, groupes et rôles), puis de détacher la politique obsolète de ces identités.

Les caractéristiques d'une politique obsolète sont les suivantes :

- Il est supprimé de ce guide.
- Les autorisations continuent de fonctionner pour toutes les identités actuellement associées.
- Dans les comptes où la politique est associée à une identité, elle apparaît dans la liste des politiques de la console IAM avec une icône d'avertissement à côté.
- Il ne peut être rattaché à aucune nouvelle identité. Si vous le détachez d'une identité actuelle, vous ne pouvez pas le rattacher.
- Une fois que vous l'avez détaché de toutes les entités actuelles, il n'est plus visible.

AWS politiques gérées

AWS politiques gérées

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

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

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

- [AmazonDetectiveOrganizationsAccess](#)
- [AmazonDetectiveServiceLinkedRolePolicy](#)
- [AmazonDevOpsGuruConsoleFullAccess](#)
- [AmazonDevOpsGuruFullAccess](#)
- [AmazonDevOpsGuruOrganizationsAccess](#)
- [AmazonDevOpsGuruReadOnlyAccess](#)
- [AmazonDevOpsGuruServiceRolePolicy](#)
- [AmazonDMSCloudWatchLogsRole](#)
- [AmazonDMSRedshiftS3Role](#)
- [AmazonDMSVPCManagementRole](#)
- [AmazonDocDB-ElasticServiceRolePolicy](#)
- [AmazonDocDBConsoleFullAccess](#)
- [AmazonDocDBElasticFullAccess](#)
- [AmazonDocDBElasticReadOnlyAccess](#)
- [AmazonDocDBFullAccess](#)
- [AmazonDocDBReadOnlyAccess](#)
- [AmazonDRSVPCManagement](#)
- [AmazonDynamoDBFullAccess](#)
- [AmazonDynamoDBFullAccesswithDataPipeline](#)
- [AmazonDynamoDBReadOnlyAccess](#)
- [AmazonEBSCSIDriverPolicy](#)
- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AmazonEC2ContainerServiceAutoscaleRole](#)
- [AmazonEC2ContainerServiceEventsRole](#)
- [AmazonEC2ContainerServiceforEC2Role](#)
- [AmazonEC2ContainerServiceRole](#)
- [AmazonEC2FullAccess](#)

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

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

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

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

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

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

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

- [AmazonRDSCustomServiceRolePolicy](#)
- [AmazonRDSDataFullAccess](#)
- [AmazonRDSDirectoryServiceAccess](#)
- [AmazonRDSEnhancedMonitoringRole](#)
- [AmazonRDSFullAccess](#)
- [AmazonRDSPerformanceInsightsFullAccess](#)
- [AmazonRDSPerformanceInsightsReadOnly](#)
- [AmazonRDSPreviewServiceRolePolicy](#)
- [AmazonRDSReadOnlyAccess](#)
- [AmazonRDSServiceRolePolicy](#)
- [AmazonRedshiftAllCommandsFullAccess](#)
- [AmazonRedshiftDataFullAccess](#)
- [AmazonRedshiftFullAccess](#)
- [AmazonRedshiftQueryEditor](#)
- [AmazonRedshiftQueryEditorV2FullAccess](#)
- [AmazonRedshiftQueryEditorV2NoSharing](#)
- [AmazonRedshiftQueryEditorV2ReadSharing](#)
- [AmazonRedshiftQueryEditorV2ReadWriteSharing](#)
- [AmazonRedshiftReadOnlyAccess](#)
- [AmazonRedshiftServiceLinkedRolePolicy](#)
- [AmazonRekognitionCustomLabelsFullAccess](#)
- [AmazonRekognitionFullAccess](#)
- [AmazonRekognitionReadOnlyAccess](#)
- [AmazonRekognitionServiceRole](#)
- [AmazonRoute53AutoNamingFullAccess](#)
- [AmazonRoute53AutoNamingReadOnlyAccess](#)
- [AmazonRoute53AutoNamingRegistrantAccess](#)
- [AmazonRoute53DomainsFullAccess](#)
- [AmazonRoute53DomainsReadOnlyAccess](#)

- [AmazonRoute53FullAccess](#)
- [AmazonRoute53ReadOnlyAccess](#)
- [AmazonRoute53RecoveryClusterFullAccess](#)
- [AmazonRoute53RecoveryClusterReadOnlyAccess](#)
- [AmazonRoute53RecoveryControlConfigFullAccess](#)
- [AmazonRoute53RecoveryControlConfigReadOnlyAccess](#)
- [AmazonRoute53RecoveryReadinessFullAccess](#)
- [AmazonRoute53RecoveryReadinessReadOnlyAccess](#)
- [AmazonRoute53ResolverFullAccess](#)
- [AmazonRoute53ResolverReadOnlyAccess](#)
- [AmazonS3FullAccess](#)
- [AmazonS3ObjectLambdaExecutionRolePolicy](#)
- [AmazonS3OutpostsFullAccess](#)
- [AmazonS3OutpostsReadOnlyAccess](#)
- [AmazonS3ReadOnlyAccess](#)
- [AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy](#)
- [AmazonSageMakerCanvasAIServicesAccess](#)
- [AmazonSageMakerCanvasBedrockAccess](#)
- [AmazonSageMakerCanvasDataPrepFullAccess](#)
- [AmazonSageMakerCanvasDirectDeployAccess](#)
- [AmazonSageMakerCanvasForecastAccess](#)
- [AmazonSageMakerCanvasFullAccess](#)
- [AmazonSageMakerClusterInstanceRolePolicy](#)
- [AmazonSageMakerCoreServiceRolePolicy](#)
- [AmazonSageMakerEdgeDeviceFleetPolicy](#)
- [AmazonSageMakerFeatureStoreAccess](#)
- [AmazonSageMakerFullAccess](#)
- [AmazonSageMakerGeospatialExecutionRole](#)
- [AmazonSageMakerGeospatialFullAccess](#)

- [AmazonSageMakerGroundTruthExecution](#)
- [AmazonSageMakerMechanicalTurkAccess](#)
- [AmazonSageMakerModelGovernanceUseAccess](#)
- [AmazonSageMakerModelRegistryFullAccess](#)
- [AmazonSageMakerNotebooksServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy](#)
- [AmazonSageMakerPipelinesIntegrations](#)
- [AmazonSageMakerReadOnly](#)
- [AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy](#)
- [AmazonSecurityLakeAdministrator](#)
- [AmazonSecurityLakeMetastoreManager](#)
- [AmazonSecurityLakePermissionsBoundary](#)
- [AmazonSESEFullAccess](#)
- [AmazonSESReadOnlyAccess](#)
- [AmazonSNSFullAccess](#)
- [AmazonSNSReadOnlyAccess](#)
- [AmazonSNSRole](#)
- [AmazonSQSFullAccess](#)
- [AmazonSQSReadOnlyAccess](#)
- [AmazonSSMAutomationApproverAccess](#)

- [AmazonSSMAutomationRole](#)
- [AmazonSSMDirectoryServiceAccess](#)
- [AmazonSSMFullAccess](#)
- [AmazonSSMMaintenanceWindowRole](#)
- [AmazonSSMManagedEC2InstanceDefaultPolicy](#)
- [AmazonSSMManagedInstanceCore](#)
- [AmazonSSMPatchAssociation](#)
- [AmazonSSMReadOnlyAccess](#)
- [AmazonSSMServiceRolePolicy](#)
- [AmazonSumerianFullAccess](#)
- [AmazonTextractFullAccess](#)
- [AmazonTextractServiceRole](#)
- [AmazonTimestreamConsoleFullAccess](#)
- [AmazonTimestreamFullAccess](#)
- [AmazonTimestreamInfluxDBFullAccess](#)
- [AmazonTimestreamInfluxDBServiceRolePolicy](#)
- [AmazonTimestreamReadOnlyAccess](#)
- [AmazonTranscribeFullAccess](#)
- [AmazonTranscribeReadOnlyAccess](#)
- [AmazonVPCCrossAccountNetworkInterfaceOperations](#)
- [AmazonVPCFullAccess](#)
- [AmazonVPCNetworkAccessAnalyzerFullAccessPolicy](#)
- [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)
- [AmazonVPCReachabilityAnalyzerPathComponentReadPolicy](#)
- [AmazonVPCReadOnlyAccess](#)
- [AmazonWorkDocsFullAccess](#)
- [AmazonWorkDocsReadOnlyAccess](#)
- [AmazonWorkMailEventsServiceRolePolicy](#)
- [AmazonWorkMailFullAccess](#)

- [AmazonWorkMailMessageFlowFullAccess](#)
- [AmazonWorkMailMessageFlowReadOnlyAccess](#)
- [AmazonWorkMailReadOnlyAccess](#)
- [AmazonWorkSpacesAdmin](#)
- [AmazonWorkSpacesApplicationManagerAdminAccess](#)
- [AmazonWorkspacesPCAAccess](#)
- [AmazonWorkSpacesSelfServiceAccess](#)
- [AmazonWorkSpacesServiceAccess](#)
- [AmazonWorkSpacesWebReadOnly](#)
- [AmazonWorkSpacesWebServiceRolePolicy](#)
- [AmazonZocaloFullAccess](#)
- [AmazonZocaloReadOnlyAccess](#)
- [AmplifyBackendDeployFullAccess](#)
- [APIGatewayServiceRolePolicy](#)
- [AppIntegrationsServiceLinkedRolePolicy](#)
- [ApplicationAutoScalingForAmazonAppStreamAccess](#)
- [ApplicationDiscoveryServiceContinuousExportServiceRolePolicy](#)
- [AppRunnerNetworkingServiceRolePolicy](#)
- [AppRunnerServiceRolePolicy](#)
- [AutoScalingConsoleFullAccess](#)
- [AutoScalingConsoleReadOnlyAccess](#)
- [AutoScalingFullAccess](#)
- [AutoScalingNotificationAccessRole](#)
- [AutoScalingReadOnlyAccess](#)
- [AutoScalingServiceRolePolicy](#)
- [AWS_ConfigRole](#)
- [AWSAccountActivityAccess](#)
- [AWSAccountManagementFullAccess](#)
- [AWSAccountManagementReadOnlyAccess](#)

- [AWSAccountUsageReportAccess](#)
- [AWSAgentlessDiscoveryService](#)
- [AWSAppFabricFullAccess](#)
- [AWSAppFabricReadOnlyAccess](#)
- [AWSAppFabricServiceRolePolicy](#)
- [AWSApplicationAutoscalingAppStreamFleetPolicy](#)
- [AWSApplicationAutoscalingCassandraTablePolicy](#)
- [AWSApplicationAutoscalingComprehendEndpointPolicy](#)
- [AWSApplicationAutoScalingCustomResourcePolicy](#)
- [AWSApplicationAutoscalingDynamoDBTablePolicy](#)
- [AWSApplicationAutoscalingEC2SpotFleetRequestPolicy](#)
- [AWSApplicationAutoscalingECSServicePolicy](#)
- [AWSApplicationAutoscalingElastiCacheRGPPolicy](#)
- [AWSApplicationAutoscalingEMRInstanceGroupPolicy](#)
- [AWSApplicationAutoscalingKafkaClusterPolicy](#)
- [AWSApplicationAutoscalingLambdaConcurrencyPolicy](#)
- [AWSApplicationAutoscalingNeptuneClusterPolicy](#)
- [AWSApplicationAutoscalingRDSClusterPolicy](#)
- [AWSApplicationAutoscalingSageMakerEndpointPolicy](#)
- [AWSApplicationDiscoveryAgentAccess](#)
- [AWSApplicationDiscoveryAgentlessCollectorAccess](#)
- [AWSApplicationDiscoveryServiceFullAccess](#)
- [AWSApplicationMigrationAgentInstallationPolicy](#)
- [AWSApplicationMigrationAgentPolicy](#)
- [AWSApplicationMigrationAgentPolicy_v2](#)
- [AWSApplicationMigrationConversionServerPolicy](#)
- [AWSApplicationMigrationEC2Access](#)
- [AWSApplicationMigrationFullAccess](#)
- [AWSApplicationMigrationMGHAccess](#)

- [AWSApplicationMigrationReadOnlyAccess](#)
- [AWSApplicationMigrationReplicationServerPolicy](#)
- [AWSApplicationMigrationServiceEc2InstancePolicy](#)
- [AWSApplicationMigrationServiceRolePolicy](#)
- [AWSApplicationMigrationSSMAccess](#)
- [AWSApplicationMigrationVCenterClientPolicy](#)
- [AWSAppMeshEnvoyAccess](#)
- [AWSAppMeshFullAccess](#)
- [AWSAppMeshPreviewEnvoyAccess](#)
- [AWSAppMeshPreviewServiceRolePolicy](#)
- [AWSAppMeshReadOnly](#)
- [AWSAppMeshServiceRolePolicy](#)
- [AWSAppRunnerFullAccess](#)
- [AWSAppRunnerReadOnlyAccess](#)
- [AWSAppRunnerServicePolicyForECRAccess](#)
- [AWSAppSyncAdministrator](#)
- [AWSAppSyncInvokeFullAccess](#)
- [AWSAppSyncPushToCloudWatchLogs](#)
- [AWSAppSyncSchemaAuthor](#)
- [AWSAppSyncServiceRolePolicy](#)
- [AWSArtifactAccountSync](#)
- [AWSArtifactReportsReadOnlyAccess](#)
- [AWSArtifactServiceRolePolicy](#)
- [AWSAuditManagerAdministratorAccess](#)
- [AWSAuditManagerServiceRolePolicy](#)
- [AWSAutoScalingPlansEC2AutoScalingPolicy](#)
- [AWSBackupAuditAccess](#)
- [AWSBackupDataTransferAccess](#)
- [AWSBackupFullAccess](#)

- [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)
- [AWSBatchFullAccess](#)
- [AWSBatchServiceEventTargetRole](#)
- [AWSBatchServiceRole](#)
- [AWSBillingConductorFullAccess](#)
- [AWSBillingConductorReadOnlyAccess](#)
- [AWSBillingReadOnlyAccess](#)
- [AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#)
- [AWSBudgetsActionsWithAWSResourceControlAccess](#)
- [AWSBudgetsReadOnlyAccess](#)
- [AWSBugBustFullAccess](#)
- [AWSBugBustPlayerAccess](#)
- [AWSBugBustServiceRolePolicy](#)
- [AWSCertificateManagerFullAccess](#)
- [AWSCertificateManagerPrivateCAAuditor](#)
- [AWSCertificateManagerPrivateCAFullAccess](#)
- [AWSCertificateManagerPrivateCAPrivilegedUser](#)
- [AWSCertificateManagerPrivateCARedOnly](#)
- [AWSCertificateManagerPrivateCAUser](#)
- [AWSCertificateManagerReadOnly](#)

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

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

- [AWSCostAndUsageReportAutomationPolicy](#)
- [AWSDataExchangeFullAccess](#)
- [AWSDataExchangeProviderFullAccess](#)
- [AWSDataExchangeReadOnly](#)
- [AWSDataExchangeSubscriberFullAccess](#)
- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWSDataPipeline_FullAccess](#)
- [AWSDataPipeline_PowerUser](#)
- [AWSDataSyncDiscoveryServiceRolePolicy](#)
- [AWSDataSyncFullAccess](#)
- [AWSDataSyncReadOnlyAccess](#)
- [AWSDeepLensLambdaFunctionAccessPolicy](#)
- [AWSDeepLensServiceRolePolicy](#)
- [AWSDeepRacerAccountAdminAccess](#)
- [AWSDeepRacerCloudFormationAccessPolicy](#)
- [AWSDeepRacerDefaultMultiUserAccess](#)
- [AWSDeepRacerFullAccess](#)
- [AWSDeepRacerRoboMakerAccessPolicy](#)
- [AWSDeepRacerServiceRolePolicy](#)
- [AWSDenyAll](#)
- [AWSDeviceFarmFullAccess](#)
- [AWSDeviceFarmServiceRolePolicy](#)
- [AWSDeviceFarmTestGridServiceRolePolicy](#)
- [AWSDirectConnectFullAccess](#)
- [AWSDirectConnectReadOnlyAccess](#)
- [AWSDirectConnectServiceRolePolicy](#)
- [AWSDirectoryServiceFullAccess](#)
- [AWSDirectoryServiceReadOnlyAccess](#)

- [AWSDiscoveryContinuousExportFirehosePolicy](#)
- [AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWSDMSServerlessServiceRolePolicy](#)
- [AWSEC2CapacityReservationFleetRolePolicy](#)
- [AWSEC2FleetServiceRolePolicy](#)
- [AWSEC2SpotFleetServiceRolePolicy](#)
- [AWSEC2SpotServiceRolePolicy](#)
- [AWSECRPullThroughCache_ServiceRolePolicy](#)
- [AWSElasticBeanstalkCustomPlatformforEC2Role](#)
- [AWSElasticBeanstalkEnhancedHealth](#)
- [AWSElasticBeanstalkMaintenance](#)
- [AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy](#)
- [AWSElasticBeanstalkManagedUpdatesServiceRolePolicy](#)
- [AWSElasticBeanstalkMulticontainerDocker](#)
- [AWSElasticBeanstalkReadOnly](#)
- [AWSElasticBeanstalkRoleCore](#)
- [AWSElasticBeanstalkRoleCWL](#)
- [AWSElasticBeanstalkRoleECS](#)
- [AWSElasticBeanstalkRoleRDS](#)
- [AWSElasticBeanstalkRoleSNS](#)
- [AWSElasticBeanstalkRoleWorkerTier](#)
- [AWSElasticBeanstalkService](#)
- [AWSElasticBeanstalkServiceRolePolicy](#)
- [AWSElasticBeanstalkWebTier](#)
- [AWSElasticBeanstalkWorkerTier](#)
- [AWSElasticDisasterRecoveryAgentInstallationPolicy](#)
- [AWSElasticDisasterRecoveryAgentPolicy](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess_v2](#)
- [AWSElasticDisasterRecoveryConversionServerPolicy](#)

- [AWSElasticDisasterRecoveryCrossAccountReplicationPolicy](#)
- [AWSElasticDisasterRecoveryEc2InstancePolicy](#)
- [AWSElasticDisasterRecoveryFailbackInstallationPolicy](#)
- [AWSElasticDisasterRecoveryFailbackPolicy](#)
- [AWSElasticDisasterRecoveryLaunchActionsPolicy](#)
- [AWSElasticDisasterRecoveryNetworkReplicationPolicy](#)
- [AWSElasticDisasterRecoveryReadOnlyAccess](#)
- [AWSElasticDisasterRecoveryRecoveryInstancePolicy](#)
- [AWSElasticDisasterRecoveryReplicationServerPolicy](#)
- [AWSElasticDisasterRecoveryServiceRolePolicy](#)
- [AWSElasticDisasterRecoveryStagingAccountPolicy](#)
- [AWSElasticDisasterRecoveryStagingAccountPolicy_v2](#)
- [AWSElasticLoadBalancingClassicServiceRolePolicy](#)
- [AWSElasticLoadBalancingServiceRolePolicy](#)
- [AWSElementalMediaConvertFullAccess](#)
- [AWSElementalMediaConvertReadOnly](#)
- [AWSElementalMediaLiveFullAccess](#)
- [AWSElementalMediaLiveReadOnly](#)
- [AWSElementalMediaPackageFullAccess](#)
- [AWSElementalMediaPackageReadOnly](#)
- [AWSElementalMediaPackageV2FullAccess](#)
- [AWSElementalMediaPackageV2ReadOnly](#)
- [AWSElementalMediaStoreFullAccess](#)
- [AWSElementalMediaStoreReadOnly](#)
- [AWSElementalMediaTailorFullAccess](#)
- [AWSElementalMediaTailorReadOnly](#)
- [AWSEnhancedClassicNetworkingMangementPolicy](#)
- [AWSEntityResolutionConsoleFullAccess](#)
- [AWSEntityResolutionConsoleReadOnlyAccess](#)
- [AWSFaultInjectionSimulatorEC2Access](#)

- [AWSFaultInjectionSimulatorECSAccess](#)
- [AWSFaultInjectionSimulatorEKSAccess](#)
- [AWSFaultInjectionSimulatorNetworkAccess](#)
- [AWSFaultInjectionSimulatorRDSAccess](#)
- [AWSFaultInjectionSimulatorSSMAccess](#)
- [AWSFinSpaceServiceRolePolicy](#)
- [AWSFMAdminFullAccess](#)
- [AWSFMAdminReadOnlyAccess](#)
- [AWSFMMemberReadOnlyAccess](#)
- [AWSForWordPressPluginPolicy](#)
- [AWSGitSyncServiceRolePolicy](#)
- [AWSGlobalAcceleratorSLRPolicy](#)
- [AWSGlueConsoleFullAccess](#)
- [AWSGlueConsoleSageMakerNotebookFullAccess](#)
- [AwsGlueDataBrewFullAccessPolicy](#)
- [AWSGlueDataBrewServiceRole](#)
- [AWSGlueSchemaRegistryFullAccess](#)
- [AWSGlueSchemaRegistryReadOnlyAccess](#)
- [AWSGlueServiceNotebookRole](#)
- [AWSGlueServiceRole](#)
- [AwsGlueSessionUserRestrictedNotebookPolicy](#)
- [AwsGlueSessionUserRestrictedNotebookServiceRole](#)
- [AwsGlueSessionUserRestrictedPolicy](#)
- [AwsGlueSessionUserRestrictedServiceRole](#)
- [AWSGrafanaAccountAdministrator](#)
- [AWSGrafanaConsoleReadOnlyAccess](#)
- [AWSGrafanaWorkspacePermissionManagement](#)
- [AWSGrafanaWorkspacePermissionManagementV2](#)
- [AWSGreengrassFullAccess](#)
- [AWSGreengrassReadOnlyAccess](#)

- [AWSGreengrassResourceAccessRolePolicy](#)
- [AWSGroundStationAgentInstancePolicy](#)
- [AWSHealth_EventProcessorServiceRolePolicy](#)
- [AWSHealthFullAccess](#)
- [AWSHealthImagingFullAccess](#)
- [AWSHealthImagingReadOnlyAccess](#)
- [AWSIAMIdentityCenterAllowListForIdentityContext](#)
- [AWSIdentitySyncFullAccess](#)
- [AWSIdentitySyncReadOnlyAccess](#)
- [AWSImageBuilderFullAccess](#)
- [AWSImageBuilderReadOnlyAccess](#)
- [AWSImportExportFullAccess](#)
- [AWSImportExportReadOnlyAccess](#)
- [AWSIncidentManagerIncidentAccessServiceRolePolicy](#)
- [AWSIncidentManagerResolverAccess](#)
- [AWSIncidentManagerServiceRolePolicy](#)
- [AWSIoT1ClickFullAccess](#)
- [AWSIoT1ClickReadOnlyAccess](#)
- [AWSIoTAnalyticsFullAccess](#)
- [AWSIoTAnalyticsReadOnlyAccess](#)
- [AWSIoTConfigAccess](#)
- [AWSIoTConfigReadOnlyAccess](#)
- [AWSIoTDataAccess](#)
- [AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction](#)
- [AWSIoTDeviceDefenderAudit](#)
- [AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction](#)
- [AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction](#)
- [AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateCACertMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction](#)

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

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

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

- [AWSMigrationHubStrategyCollector](#)
- [AWSMigrationHubStrategyConsoleFullAccess](#)
- [AWSMigrationHubStrategyServiceRolePolicy](#)
- [AWSMobileHub_FullAccess](#)
- [AWSMobileHub_ReadOnly](#)
- [AWSMSKReplicatorExecutionRole](#)
- [AWSNetworkFirewallServiceRolePolicy](#)
- [AWSNetworkManagerCloudWANServiceRolePolicy](#)
- [AWSNetworkManagerFullAccess](#)
- [AWSNetworkManagerReadOnlyAccess](#)
- [AWSNetworkManagerServiceRolePolicy](#)
- [AWSOpsWorks_FullAccess](#)
- [AWSOpsWorksCloudWatchLogs](#)
- [AWSOpsWorksCMInstanceProfileRole](#)
- [AWSOpsWorksCMServiceRole](#)
- [AWSOpsWorksInstanceRegistration](#)
- [AWSOpsWorksRegisterCLI_EC2](#)
- [AWSOpsWorksRegisterCLI_OnPremises](#)
- [AWSOrganizationsFullAccess](#)
- [AWSOrganizationsReadOnlyAccess](#)
- [AWSOrganizationsServiceTrustPolicy](#)
- [AWSOutpostsAuthorizeServerPolicy](#)
- [AWSOutpostsServiceRolePolicy](#)
- [AWSPanoramaApplianceRolePolicy](#)
- [AWSPanoramaApplianceServiceRolePolicy](#)
- [AWSPanoramaFullAccess](#)
- [AWSPanoramaGreengrassGroupRolePolicy](#)
- [AWSPanoramaSageMakerRolePolicy](#)
- [AWSPanoramaServiceLinkedRolePolicy](#)
- [AWSPanoramaServiceRolePolicy](#)

- [AWSPriceListServiceFullAccess](#)
- [AWSPriateCAAuditor](#)
- [AWSPriateCAFullAccess](#)
- [AWSPriateCAPrivilegedUser](#)
- [AWSPriateCAReadOnly](#)
- [AWSPriateCAUser](#)
- [AWSPriateMarketplaceAdminFullAccess](#)
- [AWSPriateMarketplaceRequests](#)
- [AWSPriateNetworksServiceRolePolicy](#)
- [AWSProtonCodeBuildProvisioningBasicAccess](#)
- [AWSProtonCodeBuildProvisioningServiceRolePolicy](#)
- [AWSProtonDeveloperAccess](#)
- [AWSProtonFullAccess](#)
- [AWSProtonReadOnlyAccess](#)
- [AWSProtonServiceGitSyncServiceRolePolicy](#)
- [AWSProtonSyncServiceRolePolicy](#)
- [AWSPurchaseOrdersServiceRolePolicy](#)
- [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](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMSserviceRolePolicy](#)
- [AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy](#)
- [AWSServiceRoleForCodeGuru-Profiler](#)
- [AWSServiceRoleForCodeWhispererPolicy](#)
- [AWSServiceRoleForEC2ScheduledInstances](#)
- [AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy](#)
- [AWSServiceRoleForImageBuilder](#)
- [AWSServiceRoleForIoTSiteWise](#)
- [AWSServiceRoleForLogDeliveryPolicy](#)
- [AWSServiceRoleForMonitronPolicy](#)
- [AWSServiceRoleForNeptuneGraphPolicy](#)
- [AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWSServiceRoleForSMS](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)
- [AWSShieldDRTAccessPolicy](#)
- [AWSShieldServiceRolePolicy](#)
- [AWSSSMForSAPServiceLinkedRolePolicy](#)
- [AWSSSMOpsInsightsServiceRolePolicy](#)
- [AWSSSODirectoryAdministrator](#)
- [AWSSSODirectoryReadOnly](#)
- [AWSSSOMasterAccountAdministrator](#)
- [AWSSSOMemberAccountAdministrator](#)
- [AWSSSOReadOnly](#)
- [AWSSSOServiceRolePolicy](#)
- [AWSSStepFunctionsConsoleFullAccess](#)
- [AWSSStepFunctionsFullAccess](#)

- [AWSStepFunctionsReadOnlyAccess](#)
- [AWSStorageGatewayFullAccess](#)
- [AWSStorageGatewayReadOnlyAccess](#)
- [AWSStorageGatewayServiceRolePolicy](#)
- [AWSSupplyChainFederationAdminAccess](#)
- [AWSSupportAccess](#)
- [AWSSupportAppFullAccess](#)
- [AWSSupportAppReadOnlyAccess](#)
- [AWSSupportPlansFullAccess](#)
- [AWSSupportPlansReadOnlyAccess](#)
- [AWSSupportServiceRolePolicy](#)
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSSystemsManagerChangeManagementServicePolicy](#)
- [AWSSystemsManagerForSAPFullAccess](#)
- [AWSSystemsManagerForSAPReadOnlyAccess](#)
- [AWSSystemsManagerOpsDataSyncServiceRolePolicy](#)
- [AWSThinkboxAssetServerPolicy](#)
- [AWSThinkboxAWSPortalAdminPolicy](#)
- [AWSThinkboxAWSPortalGatewayPolicy](#)
- [AWSThinkboxAWSPortalWorkerPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAccessPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginWorkerPolicy](#)
- [AWSTransferConsoleFullAccess](#)
- [AWSTransferFullAccess](#)
- [AWSTransferLoggingAccess](#)
- [AWSTransferReadOnlyAccess](#)
- [AWSTrustedAdvisorPriorityFullAccess](#)
- [AWSTrustedAdvisorPriorityReadOnlyAccess](#)

- [AWSTrustedAdvisorReportingServiceRolePolicy](#)
- [AWSTrustedAdvisorServiceRolePolicy](#)
- [AWSUserNotificationsServiceLinkedRolePolicy](#)
- [AWSVendorInsightsAssessorFullAccess](#)
- [AWSVendorInsightsAssessorReadOnly](#)
- [AWSVendorInsightsVendorFullAccess](#)
- [AWSVendorInsightsVendorReadOnly](#)
- [AWSVpcLatticeServiceRolePolicy](#)
- [AWSVPCS2SVpnServiceRolePolicy](#)
- [AWSVPCTransitGatewayServiceRolePolicy](#)
- [AWSVPCVerifiedAccessServiceRolePolicy](#)
- [AWSWAFConsoleFullAccess](#)
- [AWSWAFConsoleReadOnlyAccess](#)
- [AWSWAFFullAccess](#)
- [AWSWAFReadOnlyAccess](#)
- [AWSWellArchitectedDiscoveryServiceRolePolicy](#)
- [AWSWellArchitectedOrganizationsServiceRolePolicy](#)
- [AWSWickrFullAccess](#)
- [AWSXrayCrossAccountSharingConfiguration](#)
- [AWSXRayDaemonWriteAccess](#)
- [AWSXrayFullAccess](#)
- [AWSXrayReadOnlyAccess](#)
- [AWSXrayWriteOnlyAccess](#)
- [AWSZonalAutoshiftPracticeRunSLRPolicy](#)
- [BatchServiceRolePolicy](#)
- [Billing](#)
- [CertificateManagerServiceRolePolicy](#)
- [ClientVPNServiceConnectionsRolePolicy](#)
- [ClientVPNServiceRolePolicy](#)
- [CloudFormationStackSetsOrgAdminServiceRolePolicy](#)

- [CloudFormationStackSetsOrgMemberServiceRolePolicy](#)
- [CloudFrontFullAccess](#)
- [CloudFrontReadOnlyAccess](#)
- [CloudHSMServiceRolePolicy](#)
- [CloudSearchFullAccess](#)
- [CloudSearchReadOnlyAccess](#)
- [CloudTrailServiceRolePolicy](#)
- [CloudWatch-CrossAccountAccess](#)
- [CloudWatchActionsEC2Access](#)
- [CloudWatchAgentAdminPolicy](#)
- [CloudWatchAgentServerPolicy](#)
- [CloudWatchApplicationInsightsFullAccess](#)
- [CloudWatchApplicationInsightsReadOnlyAccess](#)
- [CloudwatchApplicationInsightsServiceLinkedRolePolicy](#)
- [CloudWatchApplicationSignalsServiceRolePolicy](#)
- [CloudWatchAutomaticDashboardsAccess](#)
- [CloudWatchCrossAccountSharingConfiguration](#)
- [CloudWatchEventsBuiltInTargetExecutionAccess](#)
- [CloudWatchEventsFullAccess](#)
- [CloudWatchEventsInvocationAccess](#)
- [CloudWatchEventsReadOnlyAccess](#)
- [CloudWatchEventsServiceRolePolicy](#)
- [CloudWatchFullAccess](#)
- [CloudWatchFullAccessV2](#)
- [CloudWatchInternetMonitorServiceRolePolicy](#)
- [CloudWatchLambdaInsightsExecutionRolePolicy](#)
- [CloudWatchLogsCrossAccountSharingConfiguration](#)
- [CloudWatchLogsFullAccess](#)
- [CloudWatchLogsReadOnlyAccess](#)
- [CloudWatchNetworkMonitorServiceRolePolicy](#)

- [CloudWatchReadOnlyAccess](#)
- [CloudWatchSyntheticsFullAccess](#)
- [CloudWatchSyntheticsReadOnlyAccess](#)
- [ComprehendDataAccessRolePolicy](#)
- [ComprehendFullAccess](#)
- [ComprehendMedicalFullAccess](#)
- [ComprehendReadOnly](#)
- [ComputeOptimizerReadOnlyAccess](#)
- [ComputeOptimizerServiceRolePolicy](#)
- [ConfigConformsServiceRolePolicy](#)
- [CostOptimizationHubAdminAccess](#)
- [CostOptimizationHubReadOnlyAccess](#)
- [CostOptimizationHubServiceRolePolicy](#)
- [CustomerProfilesServiceLinkedRolePolicy](#)
- [DatabaseAdministrator](#)
- [DataScientist](#)
- [DAXServiceRolePolicy](#)
- [DynamoDBCloudWatchContributorInsightsServiceRolePolicy](#)
- [DynamoDBKinesisReplicationServiceRolePolicy](#)
- [DynamoDBReplicationServiceRolePolicy](#)
- [EC2FastLaunchServiceRolePolicy](#)
- [EC2FleetTimeShiftableServiceRolePolicy](#)
- [Ec2ImageBuilderCrossAccountDistributionAccess](#)
- [EC2ImageBuilderLifecycleExecutionPolicy](#)
- [EC2InstanceConnect](#)
- [Ec2InstanceConnectEndpoint](#)
- [EC2InstanceProfileForImageBuilder](#)
- [EC2InstanceProfileForImageBuilderECRContainerBuilds](#)
- [ECRReplicationServiceRolePolicy](#)
- [ElastiCacheServiceRolePolicy](#)

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

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

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

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

AccessAnalyzerServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Access Analyzer à analyser les métadonnées des ressources

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 2 décembre 2019, 17:13 UTC
- Heure modifiée : 22 janvier 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

```
"lambda:GetFunctionUrlConfig",
"lambda:GetLayerVersionPolicy",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lambda:ListVersionsByFunction",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:DescribeOrganizationalUnit",
"organizations:ListAccounts",
"organizations:ListAccountsForParent",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListChildren",
"organizations:ListDelegatedAdministrators",
"organizations:ListOrganizationalUnitsForParent",
"organizations:ListParents",
"organizations:ListRoots",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketAcl",
"s3:GetBucketLocation",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPolicy",
"s3:GetBucketPublicAccessBlock",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListMultiRegionAccessPoints",
"s3express:GetBucketPolicy",
"s3express:ListAllMyDirectoryBuckets",
"sns:GetTopicAttributes",
"sns:ListTopics",
"secretsmanager:DescribeSecret",
```

```
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:ListSecrets",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AdministratorAccess

AdministratorAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux AWS services et aux ressources.

Utilisation de cette politique

Vous pouvez vous associer AdministratorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 février 2015, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AdministratorAccess-Amplify

AdministratorAccess-Amplify est une [politique AWS gérée](#) qui : accorde des autorisations administratives au compte tout en autorisant explicitement un accès direct aux ressources nécessaires aux applications Amplify.

Utilisation de cette stratégie

Vous pouvez l'associer AdministratorAccess-Amplify à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 décembre 2020, 19:03 UTC
- Heure modifiée : 31 mai 2023, 17:08 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-Amplify

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

```
"iam:TagRole",
"iam:AttachRolePolicy",
"iam:CreatePolicy",
"iam>DeletePolicy",
"iam>DeleteRole",
"iam>DeleteRolePolicy",
"iam:DetachRolePolicy",
"iam:PutRolePolicy",
"iam:UntagRole",
"iam:UpdateRole",
"iam:GetRole",
"iam:GetPolicy",
"iam:GetRolePolicy",
"iam:PassRole",
"iam:ListPolicyVersions",
"iam:CreatePolicyVersion",
"iam>DeletePolicyVersion",
"iam:CreateRole",
"iam:ListRolePolicies",
"iam:PutRolePermissionsBoundary",
"iam>DeleteRolePermissionsBoundary",
"appsync:CreateApiKey",
"appsync:CreateDataSource",
"appsync:CreateFunction",
"appsync:CreateResolver",
"appsync:CreateType",
"appsync>DeleteApiKey",
"appsync>DeleteDataSource",
"appsync>DeleteFunction",
"appsync>DeleteResolver",
"appsync>DeleteType",
"appsync:GetDataSource",
"appsync:GetFunction",
"appsync:GetIntrospectionSchema",
"appsync:GetResolver",
"appsync:GetSchemaCreationStatus",
"appsync:GetType",
"appsync:GraphQL",
"appsync:ListApiKeys",
"appsync:ListDataSources",
"appsync:ListFunctions",
"appsync:ListGraphQLApis",
"appsync:ListResolvers",
"appsync:ListResolversByFunction",
```

```
"appsync:ListTypes",
"appsync:StartSchemaCreation",
"appsync:UntagResource",
"appsync:UpdateApiKey",
"appsync:UpdateDataSource",
"appsync:UpdateFunction",
"appsync:UpdateResolver",
"appsync:UpdateType",
"appsync:TagResource",
"appsync:CreateGraphQLApi",
"appsync>DeleteGraphQLApi",
"appsync:GetGraphQLApi",
"appsync:ListTagsForResource",
"appsync:UpdateGraphQLApi",
"apigateway:DELETE",
"apigateway:GET",
"apigateway:PATCH",
"apigateway:POST",
"apigateway:PUT",
"cognito-idp:CreateUserPool",
"cognito-identity:CreateIdentityPool",
"cognito-identity>DeleteIdentityPool",
"cognito-identity:DescribeIdentity",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:SetIdentityPoolRoles",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:UpdateIdentityPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp>DeleteUserPool",
"cognito-idp>DeleteUserPoolClient",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:UpdateUserPoolClient",
"cognito-idp:CreateGroup",
"cognito-idp>DeleteGroup",
"cognito-identity:TagResource",
"cognito-idp:TagResource",
"cognito-idp:UpdateUserPool",
"cognito-idp:SetUserPoolMfaConfig",
"lambda:AddPermission",
"lambda:CreateFunction",
"lambda>DeleteFunction",
```

```
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:InvokeAsync",
"lambda:InvokeFunction",
"lambda:RemovePermission",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"lambda:ListTags",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:AddLayerVersionPermission",
"lambda:CreateEventSourceMapping",
"lambda>DeleteEventSourceMapping",
"lambda>DeleteLayerVersion",
"lambda:GetEventSourceMapping",
"lambda:GetLayerVersion",
"lambda:ListEventSourceMappings",
"lambda:ListLayerVersions",
"lambda:PublishLayerVersion",
"lambda:RemoveLayerVersionPermission",
"lambda:UpdateEventSourceMapping",
"dynamodb:CreateTable",
"dynamodb>DeleteItem",
"dynamodb>DeleteTable",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListStreams",
"dynamodb:PutItem",
"dynamodb:TagResource",
"dynamodb:ListTagsOfResource",
"dynamodb:UntagResource",
"dynamodb:UpdateContinuousBackups",
"dynamodb:UpdateItem",
"dynamodb:UpdateTable",
"dynamodb:UpdateTimeToLive",
"s3:CreateBucket",
"s3:ListBucket",
"s3:PutBucketAcl",
"s3:PutBucketCORS",
"s3:PutBucketNotification",
"s3:PutBucketPolicy",
"s3:PutBucketWebsite",
"s3:PutObjectAcl",
```

```

    "cloudfront:CreateCloudFrontOriginAccessIdentity",
    "cloudfront:CreateDistribution",
    "cloudfront>DeleteCloudFrontOriginAccessIdentity",
    "cloudfront>DeleteDistribution",
    "cloudfront:GetCloudFrontOriginAccessIdentity",
    "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:TagResource",
    "cloudfront:UntagResource",
    "cloudfront:UpdateCloudFrontOriginAccessIdentity",
    "cloudfront:UpdateDistribution",
    "events>DeleteRule",
    "events:DescribeRule",
    "events:ListRuleNamesByTarget",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "mobiletargeting:GetApp",
    "kinesis:AddTagsToStream",
    "kinesis:CreateStream",
    "kinesis>DeleteStream",
    "kinesis:DescribeStream",
    "kinesis:DescribeStreamSummary",
    "kinesis:ListTagsForStream",
    "kinesis:PutRecords",
    "es:AddTags",
    "es:CreateElasticsearchDomain",
    "es>DeleteElasticsearchDomain",
    "es:DescribeElasticsearchDomain",
    "es:UpdateElasticsearchDomainConfig",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{

```

```
"Sid" : "CLISDKCalls",
"Effect" : "Allow",
"Action" : [
  "appsync:GetIntrospectionSchema",
  "appsync:GraphQL",
  "appsync:UpdateApiKey",
  "appsync:ListApiKeys",
  "amplify:*",
  "amplifybackend:*",
  "amplifyuibuilder:*",
  "sts:AssumeRole",
  "mobiletargeting:*",
  "cognito-idp:AdminAddUserToGroup",
  "cognito-idp:AdminCreateUser",
  "cognito-idp:CreateGroup",
  "cognito-idp>DeleteGroup",
  "cognito-idp>DeleteUser",
  "cognito-idp:ListUsers",
  "cognito-idp:AdminGetUser",
  "cognito-idp:ListUsersInGroup",
  "cognito-idp:AdminDisableUser",
  "cognito-idp:AdminRemoveUserFromGroup",
  "cognito-idp:AdminResetUserPassword",
  "cognito-idp:AdminListGroupsForUser",
  "cognito-idp:ListGroups",
  "cognito-idp:AdminListUserAuthEvents",
  "cognito-idp:AdminDeleteUser",
  "cognito-idp:AdminConfirmSignUp",
  "cognito-idp:AdminEnableUser",
  "cognito-idp:AdminUpdateUserAttributes",
  "cognito-idp:DescribeIdentityProvider",
  "cognito-idp:DescribeUserPool",
  "cognito-idp>DeleteUserPool",
  "cognito-idp:DescribeUserPoolClient",
  "cognito-idp>CreateUserPool",
  "cognito-idp>CreateUserPoolClient",
  "cognito-idp:UpdateUserPool",
  "cognito-idp:AdminSetUserPassword",
  "cognito-idp:ListUserPools",
  "cognito-idp:ListUserPoolClients",
  "cognito-idp:ListIdentityProviders",
  "cognito-idp:.GetUserPoolMfaConfig",
  "cognito-identity:GetIdentityPoolRoles",
  "cognito-identity:SetIdentityPoolRoles",
```

```
"cognito-identity:CreateIdentityPool",
"cognito-identity>DeleteIdentityPool",
"cognito-identity:ListIdentityPools",
"cognito-identity:DescribeIdentityPool",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"lambda:GetFunction",
"lambda:CreateFunction",
"lambda:AddPermission",
"lambda>DeleteFunction",
"lambda>DeleteLayerVersion",
"lambda:InvokeFunction",
"lambda:ListLayerVersions",
"iam:PutRolePolicy",
"iam:CreatePolicy",
"iam:AttachRolePolicy",
"iam:ListPolicyVersions",
"iam:ListAttachedRolePolicies",
"iam:CreateRole",
"iam:PassRole",
"iam:ListRolePolicies",
"iam>DeleteRolePolicy",
"iam:CreatePolicyVersion",
"iam>DeletePolicyVersion",
"iam>DeleteRole",
"iam:DetachRolePolicy",
"cloudformation:ListStacks",
"cloudformation:DescribeStacks",
"sns:CreateSMSSandboxPhoneNumber",
"sns:GetSMSSandboxAccountStatus",
"sns:VerifySMSSandboxPhoneNumber",
"sns>DeleteSMSSandboxPhoneNumber",
"sns:ListSMSSandboxPhoneNumbers",
"sns:ListOriginationNumbers",
"rekognition:DescribeCollection",
"logs:DescribeLogStreams",
"logs:GetLogEvents",
"lex:GetBot",
"lex:GetBuiltinIntent",
"lex:GetBuiltinIntents",
"lex:GetBuiltinSlotTypes",
"cloudformation:GetTemplateSummary",
"codecommit:GitPull",
"cloudfront:GetCloudFrontOriginAccessIdentity",
```

```
    "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
    "polly:DescribeVoices"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSMCalls",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm>DeleteParameter",
    "ssm:GetParametersByPath",
    "ssm:GetParameters",
    "ssm:GetParameter",
    "ssm>DeleteParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
},
{
  "Sid" : "GeoPowerUser",
  "Effect" : "Allow",
  "Action" : [
    "geo:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifyEcrSDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "ecr:DescribeRepositories"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifyStorageSDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteBucketPolicy",
    "s3>DeleteBucketWebsite",
    "s3>DeleteObject",
    "s3>DeleteObjectVersion",
```



```

    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutBucketAcl",
    "s3:PutBucketCORS",
    "s3:PutBucketNotification",
    "s3:PutBucketPolicy",
    "s3:PutBucketVersioning",
    "s3:PutBucketWebsite",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSRCalls",
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:CreateCloudFrontOriginAccessIdentity",
    "cloudfront:CreateDistribution",
    "cloudfront:CreateInvalidation",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListCloudFrontOriginAccessIdentities",
    "cloudfront:ListDistributions",
    "cloudfront:ListDistributionsByLambdaFunction",
    "cloudfront:ListDistributionsByWebACLId",
    "cloudfront:ListFieldLevelEncryptionConfigs",
    "cloudfront:ListFieldLevelEncryptionProfiles",
    "cloudfront:ListInvalidations",
    "cloudfront:ListPublicKeys",
    "cloudfront:ListStreamingDistributions",
    "cloudfront:UpdateDistribution",
    "cloudfront:TagResource",
    "cloudfront:UntagResource",
    "cloudfront:ListTagsForResource",
    "cloudfront>DeleteDistribution",
    "iam:AttachRolePolicy",
    "iam:CreateRole",
    "iam:CreateServiceLinkedRole",

```

```

    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:PassRole",
    "lambda:CreateFunction",
    "lambda:EnableReplication",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration",
    "lambda:ListTags",
    "lambda:TagResource",
    "lambda:UntagResource",
    "route53:ChangeResourceRecordSets",
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets",
    "s3:CreateBucket",
    "s3:GetAccelerateConfiguration",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutObject",
    "s3:PutBucketTagging",
    "s3:GetBucketTagging",
    "lambda:ListEventSourceMappings",
    "lambda:CreateEventSourceMapping",
    "iam:UpdateAssumeRolePolicy",
    "iam>DeleteRolePolicy",
    "sqs:CreateQueue",
    "sqs>DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "amplify:GetApp",
    "amplify:GetBranch",
    "amplify:UpdateApp",
    "amplify:UpdateBranch"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSRViewLogGroups",
  "Effect" : "Allow",

```

```
    "Action" : "logs:DescribeLogGroups",
    "Resource" : "arn:aws:logs:*:*:log-group:*"
  },
  {
    "Sid" : "AmplifySSRCreatelogGroup",
    "Effect" : "Allow",
    "Action" : "logs:CreateLogGroup",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
  },
  {
    "Sid" : "AmplifySSRPushLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AdministratorAccess-AWSElasticBeanstalk

AdministratorAccess-AWSElasticBeanstalk est une [politique AWS gérée](#) qui : accorde des autorisations administratives aux comptes. Permet explicitement aux développeurs et aux administrateurs d'accéder directement aux ressources dont ils ont besoin pour gérer les applications AWS Elastic Beanstalk

Utilisation de cette stratégie

Vous pouvez les associer AdministratorAccess-AWSElasticBeanstalk à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la stratégie

- Type : politiqueAWS gérée
- Heure de création : 22 janvier 2021, 19:36 UTC
- Heure modifiée : 23 mars 2023, 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",

```

```

    "ec2:CreateLaunchTemplate*",
    "ec2:CreateSecurityGroup",
    "ec2:CreateTags",
    "ec2>DeleteLaunchTemplate*",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTags",
    "ec2:Describe*",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroup*",
    "ecs:CreateCluster",
    "ecs:DeRegisterTaskDefinition",
    "ecs:Describe*",
    "ecs:List*",
    "ecs:RegisterTaskDefinition",
    "elasticbeanstalk:*",
    "elasticloadbalancing:Describe*",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListServerCertificates",
    "logs:Describe*",
    "rds:Describe*",
    "s3:ListAllMyBuckets",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:*"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
}

```

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

```

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

```

```

    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:*Rule",
      "elasticloadbalancing:*Tags",
      "elasticloadbalancing:SetRulePriorities",
      "elasticloadbalancing:SetSecurityGroups"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:*"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AddRoleToInstanceProfile",
      "iam:CreateInstanceProfile",
      "iam:CreateRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-elasticbeanstalk*",
      "arn:aws:iam:*:*:instance-profile/aws-elasticbeanstalk*"
    ]
  }
}

```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
    "Condition" : {
      "StringLike" : {
        "iam:PolicyArn" : [
          "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
          "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
        ]
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "elasticbeanstalk.amazonaws.com",
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn",
        "autoscaling.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "ecs.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling*",
    "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*",
  ]
}
```

```

    "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing*",
    "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*",
    "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "autoscaling.amazonaws.com",
        "elasticbeanstalk.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "managedupdates.elasticbeanstalk.amazonaws.com",
        "maintenance.elasticbeanstalk.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:*DBSubnetGroup",
    "rds:AuthorizeDBSecurityGroupIngress",
    "rds:CreateDBInstance",
    "rds:CreateDBSecurityGroup",
    "rds>DeleteDBInstance",
    "rds>DeleteDBSecurityGroup",
    "rds:ModifyDBInstance",
    "rds:RestoreDBInstanceFromDBSnapshot"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:*",
    "arn:aws:rds:*:*:secgrp:awseb-e-*",
    "arn:aws:rds:*:*:secgrp:eb-*",

```

```
    "arn:aws:rds:*:*:snapshot:*",
    "arn:aws:rds:*:*:subgrp:awseb-e-*",
    "arn:aws:rds:*:*:subgrp:eb-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:Delete*",
    "s3:Get*",
    "s3:Put*"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucket*",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:GetTopicAttributes",
    "sns:Publish",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:*QueueAttributes",
    "sqs:CreateQueue",
    "sqs:DeleteQueue",
    "sqs:SendMessage",
```

```
    "sqs:TagQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:awseb-e-*",
    "arn:aws:sqs:*:*:eb-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "CreateCluster",
        "RegisterTaskDefinition"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessDeviceSetup

AlexaForBusinessDeviceSetup est une [politique AWS gérée](#) qui : Fournit un accès aux AlexaForBusiness services de configuration de l'appareil

Utilisation de cette stratégie

Vous pouvez les associer `AlexaForBusinessDeviceSetup` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 20 mai 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessFullAccess

AlexaForBusinessFullAccess est une [politique AWS gérée](#) qui : Accorde un accès complet aux AlexaForBusiness ressources et l'accès aux Services AWS

Utilisation de cette stratégie

Vous pouvez AlexaForBusinessFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 01 juillet 2020, 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessGatewayExecution

AlexaForBusinessGatewayExecution est une [politiqueAWS gérée](#) qui : Fournit un accès d'exécution de la passerelle aux AlexaForBusiness services

Utilisation de cette stratégie

Vous pouvez les associer AlexaForBusinessGatewayExecution à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 30 novembre 2017, 16:47 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

```
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

AlexaForBusinessLifesizeDelegatedAccessPolicy est une [politique AWS gérée](#) qui : Fournit l'accès aux appareils Lifesize AVS

Utilisation de la présente stratégie

Vous pouvez AlexaForBusinessLifesizeDelegatedAccessPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 4 juin 2020, 19:46 UTC
- Heure modifiée : 12 juin 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "a4b:filters_deviceType" : [
        "*A2IW07UEGW4TL"
      ]
    },
    "Null" : {
      "a4b:filters_deviceType" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "a4b:AssociateDeviceWithRoom"
  ],
  "Resource" : [
    "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGW4TL",
    "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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessNetworkProfileServicePolicy

AlexaForBusinessNetworkProfileServicePolicyest une [politiqueAWS gérée](#) qui : Cette politique permet à Alexa for Business d'effectuer des tâches automatisées planifiées par vos profils réseau.

Utilisation cette politique en utilisant cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos groupes, les groupes ou les groupes ou les groupes ou les groupes ou les groupes ou les groupes ou les groupes ou

Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 mars 2019, 00:53 UTC
- Heure modifiée : 5 avril 2019, 21:57 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège préprivilège qui](#)

AlexaForBusinessPolyDelegatedAccessPolicy

AlexaForBusinessPolyDelegatedAccessPolicy est une [politique AWS gérée](#) qui : Fournit l'accès aux appareils Poly AVS

Utilisation de cette stratégie

Vous pouvez AlexaForBusinessPolyDelegatedAccessPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 16 octobre 2019, 19:48 UTC
- Heure modifiée : 16 octobre 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

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

```



```

    "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
    "arn:aws:a4b:us-east-1:*:room/*"
  ]
},
{
  "Action" : [
    "a4b:GetRoom",
    "a4b:SearchRooms",
    "a4b:CreateRoom",
    "a4b:GetProfile",
    "a4b:SearchSkillGroups",
    "a4b:DisassociateSkillGroupFromRoom",
    "a4b:AssociateSkillGroupWithRoom",
    "a4b:GetSkillGroup",
    "a4b:SearchProfiles",
    "a4b:GetAddressBook",
    "a4b:UpdateRoom"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AlexaForBusinessReadOnlyAccess

AlexaForBusinessReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux AlexaForBusiness services

Utilisation de cette stratégie

Vous pouvez AlexaForBusinessReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 20 novembre 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAPIGatewayAdministrator

AmazonAPIGatewayAdministrator est une [politiqueAWS gérée](#) qui : fournit un accès complet à la création/modification/suppression d'API dans Amazon API Gateway via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonAPIGatewayAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 juillet 2015, 17:34 UTC
- Heure modifiée : 09 juillet 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAPIGatewayInvokeFullAccess

AmazonAPIGatewayInvokeFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet pour appeler des API dans Amazon API Gateway.

Utilisation de cette stratégie

Vous pouvez AmazonAPIGatewayInvokeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 juillet 2015, 17:36 UTC
- Heure modifiée : 18 décembre 2018, 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogsest une [politiqueAWS gérée](#) qui : Autorise API Gateway à transmettre les journaux au compte de l'utilisateur.

Utilisation de cette stratégie

Vous pouvezAmazonAPIGatewayPushToCloudWatchLogs les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 novembre 2015, 23:41 UTC

- Heure modifiée : 11 novembre 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppFlowFullAccess

AmazonAppFlowFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon AppFlow et un accès aux AWS services pris en charge en tant que source ou destination de flux (S3 et Redshift). Fournit également un accès à KMS pour le chiffrement

Utilisation de cette stratégie

Vous pouvez AmazonAppFlowFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 juin 2020, 23h30 UTC
- Heure modifiée : 28 février 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "KMSListAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KMSGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "appflow.*.amazonaws.com"
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      }
    }
  },
  {
    "Sid" : "KMSListGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListGrants"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "appflow.*.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3ReadAccess",
    "Effect" : "Allow",
    "Action" : [
```



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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppFlowReadOnlyAccess

AmazonAppFlowReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux flux Amazon Appflow

Utilisation de cette stratégie

Vous pouvez AmazonAppFlowReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 juin 2020, 23:26 UTC
- Heure modifiée : 28 février 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppStreamFullAccess

AmazonAppStreamFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon AppStream via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonAppStreamFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 28 août 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
```

```

    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling>DeleteScheduledAction"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "cloudwatch>DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:PutMetricAlarm"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "iam:ListRoles",
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "application-autoscaling.amazonaws.com"
    }
  }
}

```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppStreamPCAAccess

AmazonAppStreamPCAAccess est une [politiqueAWS gérée](#) qui : Amazon AppStream 2.0 accède à l'autorité de certification privée deAWS Certificate Manager dans les comptes clients pour une authentification basée sur des certificats

Utilisation de cette stratégie

Vous pouvezAmazonAppStreamPCAAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 24 octobre 2022, 17:05 UTC

- Heure modifiée : 24 octobre 2022, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppStreamReadOnlyAccess

AmazonAppStreamReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon AppStream via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonAppStreamReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 7 décembre 2016, 21 h 00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAppStreamServiceAccess

AmazonAppStreamServiceAccess est une [politiqueAWS gérée qui : Politique](#) par défaut pour le rôle AppStream de service Amazon.

Utilisation de cette stratégie

Vous pouvez AmazonAppStreamServiceAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 novembre 2016, 04:17 UTC
- Heure modifiée : 26 juin 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeAvailabilityZones",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeSubnets",
      "ec2:AssociateAddress",
      "ec2:DisassociateAddress",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVpcEndpoints",
      "s3:ListAllMyBuckets",
      "ds:DescribeDirectories"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject",
      "s3:GetObjectVersion",
      "s3>DeleteObjectVersion",
      "s3:GetBucketPolicy",
      "s3:PutBucketPolicy",
      "s3:PutEncryptionConfiguration"
    ],
    "Resource" : [
      "arn:aws:s3:::appstream2-36fb080bb8-*",
      "arn:aws:s3:::appstream-app-settings-*",
      "arn:aws:s3:::appstream-logs-*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAthenaFullAccess

AmazonAthenaFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Athena et un accès délimité aux dépendances nécessaires pour permettre les requêtes, la rédaction des résultats et la gestion des données.

Utilisation de cette politique

Vous pouvez vous associer AmazonAthenaFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 16:46 UTC
- Heure modifiée : 3 janvier 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "BaseAthenaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseGluePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:UpdateDatabase",
    "glue:CreateTable",
    "glue>DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue:GetTable",
    "glue:GetTables",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue>DeletePartition",
    "glue:BatchDeletePartition",
    "glue:UpdatePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchGetPartition",
    "glue:StartColumnStatisticsTaskRun",
    "glue:GetColumnStatisticsTaskRun",
    "glue:GetColumnStatisticsTaskRuns"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseQueryResultsPermissions",
  "Effect" : "Allow",
```

```
"Action" : [
  "s3:GetBucketLocation",
  "s3:GetObject",
  "s3:ListBucket",
  "s3:ListBucketMultipartUploads",
  "s3:ListMultipartUploadParts",
  "s3:AbortMultipartUpload",
  "s3:CreateBucket",
  "s3:PutObject",
  "s3:PutBucketPublicAccessBlock"
],
"Resource" : [
  "arn:aws:s3:::aws-athena-query-results-*"
]
},
{
  "Sid" : "BaseAthenaExamplesPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::athena-examples*"
  ]
},
{
  "Sid" : "BaseS3BucketPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BaseSNSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:GetTopicAttributes"
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "BaseCloudWatchPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:GetMetricData"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "BaseLakeFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataAccess"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "BaseDataZonePermissions",
    "Effect" : "Allow",
    "Action" : [
      "datazone:ListDomains",
      "datazone:ListProjects",
      "datazone:ListAccountEnvironments"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "BasePricingPermissions",
    "Effect" : "Allow",
    "Action" : [
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonAugmentedAIFullAccess

AmazonAugmentedAIFullAccess est une [politique AWS gérée](#) qui : fournit un accès pour effectuer toutes les opérations, les ressources Amazon Augmented AI, y compris FlowDefinitions, HumanTaskUis et HumanLoops. N'autorise pas l'accès à la création FlowDefinitions contre le public Workteam.

Utilisation de cette stratégie

Vous pouvez AmazonAugmentedAIFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 16:21 UTC
- Heure modifiée : 3 décembre 2019, 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès permettant d'effectuer toutes les opérations sur HumanLoops.

Utilisation de cette stratégie

Vous pouvez AmazonAugmentedAIHumanLoopFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 16:20 UTC
- Heure modifiée : 3 décembre 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonAugmentedAIIntegratedAPIAccess

AmazonAugmentedAIIntegratedAPIAccess est une [politique AWS gérée](#) qui : fournit un accès pour effectuer toutes les opérations, les ressources Amazon Augmented AI, y compris FlowDefinitions, HumanTaskUis et HumanLoops. Permet également d'accéder aux opérations des services intégrés à Amazon Augmented AI.

Utilisation de cette stratégie

Vous pouvez AmazonAugmentedAIIntegratedAPIAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 22 avril 2020, 20:47 UTC
- Heure modifiée : 22 avril 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonBedrockFullAccess

AmazonBedrockFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Bedrock ainsi qu'un accès limité aux services connexes requis par celui-ci

Utilisation de cette politique

Vous pouvez vous associer `AmazonBedrockFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 décembre 2023, 15:47 UTC
- Heure modifiée : 6 décembre 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:*:*"
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonBedrockReadOnly

AmazonBedrockReadOnly est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Bedrock

Utilisation de cette politique

Vous pouvez vous associer AmazonBedrockReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 décembre 2023, 15:48 UTC
- Heure modifiée : 6 décembre 2023, 15:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonBraketFullAccess

AmazonBraketFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Braket via le SDK AWS Management Console et. Permet également d'accéder à des services connexes (par exemple, S3, journaux).

Utilisation de cette stratégie

Vous pouvez AmazonBraketFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 août 2020, 20:12 UTC
- Heure modifiée : 19 avril 2023, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Effect" : "Allow",
"Action" : [
  "logs:Describe*",
  "logs:Get*",
  "logs:List*",
  "logs:StartQuery",
  "logs:StopQuery",
  "logs:TestMetricFilter",
  "logs:FilterLogEvents"
],
"Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "iam:ListRolePolicies",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListNotebookInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreatePresignedNotebookInstanceUrl",
    "sagemaker:CreateNotebookInstance",
    "sagemaker>DeleteNotebookInstance",
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:StartNotebookInstance",
    "sagemaker:StopNotebookInstance",
    "sagemaker:UpdateNotebookInstance",
    "sagemaker:ListTags",
    "sagemaker:AddTags",
    "sagemaker>DeleteTags"
  ],
}
```

```

    "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribeNotebookInstanceLifecycleConfig",
      "sagemaker>CreateNotebookInstanceLifecycleConfig",
      "sagemaker>DeleteNotebookInstanceLifecycleConfig",
      "sagemaker>ListNotebookInstanceLifecycleConfigs",
      "sagemaker:UpdateNotebookInstanceLifecycleConfig"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
  },
  {
    "Effect" : "Allow",
    "Action" : "braket:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "braket.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "sagemaker.amazonaws.com"
        ]
      }
    }
  }
}

```

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

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicyest une [politiqueAWS gérée](#) qui : accorde l'accès auxServices AWS ressources nécessaires à l'exécution d'un Amazon Braket Job, notamment S3, Cloudwatch, IAM et Braket

Utilisation de cette stratégie

Vous pouvezAmazonBraketJobsExecutionPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 26 novembre 2021, 19:34 UTC
- Heure modifiée : 28 novembre 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",

```

```
    "braket:SearchDevices",
    "braket:SearchJobs",
    "braket:SearchQuantumTasks",
    "braket:ListTagsForResource",
    "braket:TagResource",
    "braket:UntagResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "braket.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:GetQueryResults"
  ],
  "Resource" : [
    "arn:aws:logs::*:log-group:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:PutLogEvents",
    "logs:CreateLogStream",
```

```
    "logs:CreateLogGroup",
    "logs:GetLogEvents",
    "logs:DescribeLogStreams",
    "logs:StartQuery",
    "logs:StopQuery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "/aws/braket"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonBraketServiceRolePolicy

AmazonBraketServiceRolePolicy est une [politiqueAWS gérée](#) qui : Permet à Amazon Braket de créer et de gérerAWS des ressources en votre nom

Utilisation des stratégies de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 août 2020, 17:12 UTC
- Heure modifiée : 6 août 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeFullAccess

AmazonChimeFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à la console d'administration Amazon Chime via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonChimeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 novembre 2017, 22:15 UTC
- Heure modifiée : 14 décembre 2020, 21 h 00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeReadOnly

AmazonChimeReadOnly est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à la console d'administration Amazon Chime via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonChimeReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 novembre 2017, 22:04 UTC
- Heure modifiée : 14 décembre 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Version de la politique

Version de la politique :v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",

```

```
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeSDK

AmazonChimeSDK est une [politique AWS gérée](#) qui : Fournit un accès aux opérations du SDK Amazon Chime

Utilisation de cette stratégie

Vous pouvez AmazonChimeSDK les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 4 février 2020, 21:53 UTC
- Heure modifiée : 10 janvier 2023, 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : [Politique](#) gérée pour le rôle lié au service Amazon Chime SDK MediaPipelines

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 04 avril 2022, 22:02 UTC
- Heure modifiée : 8 décembre 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à Amazon Chime SDK Messaging d'accéder aux AWS ressources et d'activer les fonctionnalités de messagerie

Utilisation des politique de politique de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, des groupes ou des rôles.

les politique de politique

- Type : Politique de rôles liée à un service
- Heure de création : 3 mars 2023, 01:43 UTC
- Heure modifiée : 3 mars 2023, 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les les stratégies de politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

politique JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [stratégiesAWS gérées et évoluer vers vers vers les autorisations de moindre privilège](#)

AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy est une [politique AWS gérée](#) qui : Permet l'accès aux AWS ressources utilisées ou gérées par Amazon Chime

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 30 septembre 2019, 22:25 UTC
- Heure modifiée : 30 septembre 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy est une [politiqueAWS gérée](#) qui :
Autorise Amazon Chime à accéder à Amazon Transcribe et Amazon Transcribe Medical en votre nom

Using this policy

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 4 août 2021, 21:47 UTC
- Heure modifiée : 4 août 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

JSON policy document

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS](#)

AmazonChimeUserManagement

AmazonChimeUserManagement est une [politique AWS gérée](#) qui : fournit un accès de gestion des utilisateurs à la console d'administration Amazon Chime via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonChimeUserManagement les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 novembre 2017, 22:17 UTC
- Heure modifiée : 18 février 2020, 19:26 UTC

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

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroup",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
```

```
    "chime:UpdateUser",
    "chime:BatchUpdateUser",
    "chime:BatchSuspendUser",
    "chime:BatchUnsuspendUser",
    "chime:AssociatePhoneNumberWithUser",
    "chime:DisassociatePhoneNumberFromUser",
    "chime:GetPhoneNumber",
    "chime:ListPhoneNumbers",
    "chime:GetUserSettings",
    "chime:UpdateUserSettings",
    "chime:CreateUser",
    "chime:AssociateSigninDelegateGroupsWithAccount",
    "chime:DisassociateSigninDelegateGroupsFromAccount"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy est une [stratégie AWS gérée](#) qui :
Stratégie gérée pour le rôle lié à un service pour Amazon Chime VoiceConnector

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 30 septembre 2019, 22:16 UTC
- Heure modifiée : 14 avril 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon Cloud Directory Service.

Utilisation de cette stratégie

Vous pouvez AmazonCloudDirectoryFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 février 2017, 00:41 UTC
- Heure modifiée : 25 février 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudDirectoryReadOnlyAccess

AmazonCloudDirectoryReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon Cloud Directory Service.

Utilisation de cette stratégie

Vous pouvez AmazonCloudDirectoryReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 février 2017, 23:42 UTC
- Heure modifiée : 28 février 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchEvidentlyFullAccess

AmazonCloudWatchEvidentlyFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet uniquement à Amazon CloudWatch Evidence. Permet également d'accéder à Amazon S3, Amazon SNS CloudWatch, Amazon et à d'autres services connexes.

Utilisation de cette stratégie

Vous pouvez AmazonCloudWatchEvidentlyFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 15:10 UTC
- Heure modifiée : 29 novembre 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

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



```
    ]
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

AmazonCloudWatchEvidentlyReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon CloudWatch Evidence

Utilisation de cette stratégie

Vous pouvez AmazonCloudWatchEvidentlyReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2021, 15:08 UTC
- Heure modifiée : 29 novembre 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

AmazonCloudWatchEvidentlyServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet à CloudWatch Evidence Service de gérer lesAWS ressources associées pour le compte du client

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 septembre 2022, 17:25 UTC
- Heure modifiée : 13 septembre 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchRUMFullAccess

AmazonCloudWatchRUMFullAccess est une [politiqueAWS gérée](#) qui : accorde des autorisations d'accès complètes au service Amazon CloudWatch RUM

Utilisation de cette stratégie

Vous pouvez AmazonCloudWatchRUMFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2021, 15:46 UTC
- Heure modifiée : 29 novembre 2021, 15:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

```

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

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess est une [politiqueAWS gérée](#) qui : accorde des autorisations en lecture seule pour le service Amazon CloudWatch RUM

Utilisation de cette stratégie

Vous pouvez les associer AmazonCloudWatchRUMReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2021, 15:43 UTC
- Heure modifiée : 28 octobre 2022, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCloudWatchRUMServiceRolePolicy

AmazonCloudWatchRUMServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon CloudWatch RUM Service à publier des données de surveillance vers d'autres AWS services concernés

Utilisation des des des des des politiques

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des des des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 novembre 2021, 23:17 UTC

- Heure modifiée : 22 février 2023, 20:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de stratégie JAM

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des des des des autorisationsAWS de moindre privilège et évoluez vers les les des autorisations de moindre privilège et évoluez vers](#)

AmazonCodeCatalystFullAccess

AmazonCodeCatalystFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à AmazonCodeCatalyst

Utilisation de cette stratégie

Vous pouvez AmazonCodeCatalystFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 20 avril 2023, 16:50 UTC
- Heure modifiée : 20 avril 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeCatalystReadOnlyAccess

AmazonCodeCatalystReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon CodeCatalyst

Utilisation de cette stratégie

Vous pouvez `AmazonCodeCatalystReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 avril 2023, 16:49 UTC
- Heure modifiée : 20 avril 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeCatalystSupportAccess

AmazonCodeCatalystSupportAccess est une [politiqueAWS gérée](#) qui : permet CodeCatalyst à Amazon de créer, de mettre à jour et de résoudreAWS Support des litiges en votre nom.

Utilisation de cette stratégie

Vous pouvezAmazonCodeCatalystSupportAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2023, 12:34 UTC
- Heure modifiée : 20 avril 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Action" : [
  "support:DescribeAttachment",
  "support:DescribeCaseAttributes",
  "support:DescribeCases",
  "support:DescribeCommunications",
  "support:DescribeIssueTypes",
  "support:DescribeServices",
  "support:DescribeSeverityLevels",
  "support:DescribeSupportLevel",
  "support:SearchForCases",
  "support:AddAttachmentsToSet",
  "support:AddCommunicationToCase",
  "support:CreateCase",
  "support:InitiateCallForCase",
  "support:InitiateChatForCase",
  "support:PutCaseAttributes",
  "support:RateCaseCommunication",
  "support:ResolveCase"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruProfilerAgentAccess

AmazonCodeGuruProfilerAgentAccess est une [politiqueAWS gérée](#) qui : Fournit l'accès requis par l'agent Amazon CodeGuru Profiler.

Utilisation de cette stratégie

Vous pouvez AmazonCodeGuruProfilerAgentAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 5 février 2021, 22:11 UTC
- Heure modifiée : 5 mai 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruProfilerFullAccess

AmazonCodeGuruProfilerFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon CodeGuru Profiler.

Utilisation de cette stratégie

Vous pouvez les associer AmazonCodeGuruProfilerFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 10:13 UTC
- Heure modifiée : 15 juillet 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
    },
  ],
}
```

```
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruProfilerReadOnlyAccess

AmazonCodeGuruProfilerReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon CodeGuru Profiler.

Utilisation de cette stratégie

Vous pouvez les associer AmazonCodeGuruProfilerReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 10h30 UTC

- Heure modifiée : 27 juin 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruReviewerFullAccess

AmazonCodeGuruReviewerFullAccess est une [politique AWS gérée](#) qui : accorde un accès complet à Amazon CodeGuru Reviewer et un accès limité aux dépendances requises.

Utilisation de cette stratégie

Vous pouvez les associer AmazonCodeGuruReviewerFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 08:33 UTC
- Heure modifiée : 29 août 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "Sid" : "AmazonCodeGuruReviewerSLRCreation",
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
  },
  {
    "Sid" : "CodeCommitAccess",
    "Effect" : "Allow",
    "Action" : [
      "codecommit:ListRepositories"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CodeCommitTagManagement",
    "Effect" : "Allow",
    "Action" : [
      "codecommit:TagResource",
      "codecommit:UntagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "codeguru-reviewer"
      }
    }
  },
  {

```

```
"Sid" : "CodeConnectTagManagement",
"Effect" : "Allow",
"Action" : [
  "codestar-connections:TagResource",
  "codestar-connections:UntagResource",
  "codestar-connections:ListTagsForResource"
],
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : "codeguru-reviewer"
  }
}
},
{
  "Sid" : "CodeConnectManagedRules",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codestar-connections:ListConnections",
    "codestar-connections:PassConnection"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "codestar-connections:ProviderAction" : [
        "ListRepositories",
        "ListOwners"
      ]
    }
  }
}
},
{
  "Sid" : "CloudWatchEventsManagedRules",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:RemoveTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
```

```
        "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"  
    }  
  }  
} ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruReviewerReadOnlyAccess

AmazonCodeGuruReviewerReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon CodeGuru Reviewer.

Utilisation de cette stratégie

Vous pouvez AmazonCodeGuruReviewerReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 08:48 UTC
- Heure modifiée : 29 août 2020, 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy est une [politique AWS gérée](#) qui : Un rôle lié à un service est requis pour qu'Amazon CodeGuru Reviewer puisse accéder aux ressources en votre nom.

Utilisation de cette politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à ce service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 3 décembre 2019, 05:31 UTC
- Heure modifiée : 27 novembre 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON Document de politique

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

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques et évoluez vers AWS les autorisations de moindre privilège privilège privilège privilège vers les autorisations de moindre privilège privilège privilège privilège](#)

AmazonCodeGuruSecurityFullAccess

AmazonCodeGuruSecurityFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AmazonCodeGuru Security.

Utilisation de cette stratégie

Vous pouvez AmazonCodeGuruSecurityFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 mai 2023, 21:03 UTC
- Heure modifiée : 09 mai 2023, 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCodeGuruSecurityScanAccess

AmazonCodeGuruSecurityScanAccess est une [politique AWS gérée](#) qui : Fournit l'accès requis pour travailler avec les scans CodeGuru de sécurité Amazon.

Utilisation de cette stratégie

Vous pouvez les associer AmazonCodeGuruSecurityScanAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 mai 2023, 20:54 UTC
- Heure modifiée : 09 mai 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    ],  
    "Resource" : "arn:aws:codeguru-security:*:*:scans/*"  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCognitoDeveloperAuthenticatedIdentities

AmazonCognitoDeveloperAuthenticatedIdentities est une [politiqueAWS gérée](#) qui : fournit un accès aux API Amazon Cognito pour prendre en charge les identités authentifiées par les développeurs à partir de votre backend d'authentification.

Utilisation de cette stratégie

Vous pouvez AmazonCognitoDeveloperAuthenticatedIdentities les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 mars 2015, 17:22 UTC
- Heure modifiée : 24 mars 2015, 17:22 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonCognitoDeveloperAuthenticatedIdentities

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCognitoIdpEmailServiceRolePolicy

AmazonCognitoIdpEmailServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise le service Amazon Cognito User Pools à utiliser vos identités SES pour l'envoi d'e-mails

Utilisation politique Utilisation cette politique ISON

Cette politique est attachée à un rôle lié à un service qui permet à ce service qui permet à ce service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à

vos utilisateurs, les utilisateurs, les utilisateurs, les utilisateurs, les utilisateurs, les utilisateurs, les utilisateurs,

détails politiques IAM

- Type : Politique de rôles liée à un service
- Heure de création : 21 mars 2019, 21:32 UTC
- Heure modifiée : 21 mars 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON

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



```
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCognitoIdpServiceRolePolicy

AmazonCognitoIdpServiceRolePolicy est une [politiqueAWS gérée](#) qui : Autorise l'accès aux groupes d'utilisateurs Amazon CognitoServices AWS et aux ressources utilisées ou gérées par ceux-ci

Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à un utilisateur, un groupe ou un rôle.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 26 juin 2020, 22h30 UTC
- Heure modifiée : 26 juin 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document

```
{
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AmazonCognitoPowerUser

AmazonCognitoPowerUser est une [politique AWS gérée](#) qui : fournit un accès administratif aux ressources Amazon Cognito existantes. Vous aurez besoin de privilèges Compte AWS d'administrateur pour créer de nouvelles ressources Cognito.

Utilisation de cette stratégie

Vous pouvez les associer AmazonCognitoPowerUser à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 mars 2015, 17:14 UTC
- Heure modifiée : 01 juin 2021, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
      "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCognitoReadOnly

AmazonCognitoReadOnly est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux ressources Amazon Cognito.

Utilisation de cette stratégie

Vous pouvez AmazonCognitoReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 mars 2015, 17:06 UTC
- Heure modifiée : 01 août 2019, 19:21 UTC

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

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

AmazonCognitoUnAuthedIdentitiesSessionPolicy est un [AWSpolitique gérée](#) cela : Cette politique définit l'ensemble des autorisations autorisées pour les identités non authentifiées pour les pools d'identités Cognito. Cette politique n'est pas destinée à être utilisée comme une politique d'autorisation autonome. Il sert de protection contre les politiques trop permissives associées aux rôles dans un pool d'identités. N'associez cette politique à aucun rôle, car Cognito Identity Service l'inclura automatiquement en tant que politique limitée lors de la création des informations d'identification. Les privilèges permettant d'accéder temporairement à d'autresAWSles ressources via le flux amélioré seront désormais définies par l'intersection du rôle associé à l'identité de l'utilisateur non authentifié fourni par un service et des privilèges accordés dans cette politique gérée qui appartient à Cognito.

Utilisation de cette politique

Vous pouvez joindreAmazonCognitoUnAuthedIdentitiesSessionPolicyà vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 19 juillet 2023, 23:04 UTC
- Heure de modification :19 juillet 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

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

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonCognitoUnauthenticatedIdentities

AmazonCognitoUnauthenticatedIdentitiesest une [politiqueAWS gérée](#) qui : Cette politique définit l'ensemble des autorisations autorisées pour les identités non authentifiées pour les pools d'identités Cognito. Il n'est pas nécessaire de l'associer à votre rôle unauth, car Cognito Identity Service l'inclura automatiquement en tant que politique limitée lors de la création des informations d'identification. Les privilèges permettant d'accéder temporairement à d'autresAWS ressources via le flux amélioré seront désormais définis par l'intersection du rôle associé à l'identité de l'utilisateur non

authentifié fourni par un service et des privilèges accordés dans cette politique gérée appartenant à Cognito.

Utilisation de cette stratégie

Vous pouvez AmazonCognitoUnauthenticatedIdentities les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 février 2023, 22:36 UTC
- Heure modifiée : 01 février 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonConnect_FullAccess

AmazonConnect_FullAccess est une [politique AWS gérée](#) qui : L'objectif de cette politique est d'accorder les autorisations nécessaires aux utilisateurs AWS Connect pour utiliser les ressources Connect. Cette politique fournit un accès complet aux ressources AWS Connect par l'intermédiaire de la console.

Utilisation de cette politique

Vous pouvez AmazonConnect_FullAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2020, 19:54 UTC
- Heure modifiée : 07 mars 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "connect:*",
    "ds:CreateAlias",
    "ds:AuthorizeApplication",
    "ds:CreateIdentityPoolDirectory",
    "ds>DeleteDirectory",
    "ds:DescribeDirectories",
    "ds:UnauthorizeApplication",
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams",
    "kinesis:DescribeStream",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lex:GetBots",
    "lex:ListBots",
    "lex:ListBotAliases",
    "logs:CreateLogGroup",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "lambda:ListFunctions",
    "ds:CheckAlias",
    "profile:ListAccountIntegrations",
    "profile:GetDomain",
    "profile:ListDomains",
    "profile:GetProfileObjectType",
    "profile:ListProfileObjectTypeTemplates"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "profile:AddProfileKey",
    "profile:CreateDomain",
    "profile:CreateProfile",
    "profile>DeleteDomain",
    "profile>DeleteIntegration",
    "profile>DeleteProfile",
    "profile>DeleteProfileKey",
    "profile>DeleteProfileObject",
    "profile>DeleteProfileObjectType",
    "profile:GetIntegration",
    "profile:GetMatches",
    "profile:GetProfileObjectType",
```

```

    "profile:ListIntegrations",
    "profile:ListProfileObjects",
    "profile:ListProfileObjectTypes",
    "profile:ListTagsForResource",
    "profile:MergeProfiles",
    "profile:PutIntegration",
    "profile:PutProfileObject",
    "profile:PutProfileObjectType",
    "profile:SearchProfiles",
    "profile:TagResource",
    "profile:UntagResource",
    "profile:UpdateDomain",
    "profile:UpdateProfile"
  ],
  "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucketAcl"
  ],
  "Resource" : "arn:aws:s3:::amazon-connect-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ],
  "Resource" : "arn:aws:servicequotas:*:*:connect/*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "connect.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam>DeleteServiceLinkedRole",

```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "profile.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

AmazonConnectCampaignsServiceLinkedRolePolicy est une [politique AWS gérée qui : Politique](#) pour le rôle lié au service Amazon Connect Campaigns

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 23 septembre 2021, 20:54 UTC
- Heure modifiée : 8 novembre 2023, 16:16 UTC

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

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonConnectReadOnlyAccess

AmazonConnectReadOnlyAccess est une [politique AWS gérée](#) qui : accorde l'autorisation de consulter les instances Amazon Connect dans votre Compte AWS.

Utilisation de cette stratégie

Vous pouvez AmazonConnectReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 octobre 2018, 21:00 UTC
- Heure modifiée : 6 novembre 2019, 22h10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Deny",
  "Action" : "connect:GetFederationTokens",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonConnectServiceLinkedRolePolicy

AmazonConnectServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : permet à Amazon Connect de créer et de gérer AWS des ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 07 septembre 2018, 00:21 UTC
- Heure modifiée : 28 novembre 2023, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



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

```

    ],
    "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
  },
  {
    "Sid" : "AllowReadPermissionForCustomerProfileObjects",
    "Effect" : "Allow",
    "Action" : [
      "profile:ListProfileObjects",
      "profile:GetProfileObjectType"
    ],
    "Resource" : [
      "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
    ]
  },
  {
    "Sid" : "AllowListIntegrationForCustomerProfile",
    "Effect" : "Allow",
    "Action" : [
      "profile:ListAccountIntegrations"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadForCustomerProfileObjectTemplates",
    "Effect" : "Allow",
    "Action" : [
      "profile:ListProfileObjectTypeTemplates",
      "profile:GetProfileObjectTypeTemplate"
    ],
    "Resource" : "arn:aws:profile:*:*:/templates*"
  },
  {
    "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
    "Effect" : "Allow",
    "Action" : [
      "wisdom:CreateContent",
      "wisdom>DeleteContent",
      "wisdom:CreateKnowledgeBase",
      "wisdom:GetAssistant",
      "wisdom:GetKnowledgeBase",
      "wisdom:GetContent",
      "wisdom:GetRecommendations",
      "wisdom:GetSession",
      "wisdom:NotifyRecommendationsReceived",

```

```

    "wisdom:QueryAssistant",
    "wisdom:StartContentUpload",
    "wisdom:UpdateContent",
    "wisdom:UntagResource",
    "wisdom:TagResource",
    "wisdom:CreateSession",
    "wisdom:CreateQuickResponse",
    "wisdom:GetQuickResponse",
    "wisdom:SearchQuickResponses",
    "wisdom:StartImportJob",
    "wisdom:GetImportJob",
    "wisdom:ListImportJobs",
    "wisdom:ListQuickResponses",
    "wisdom:UpdateQuickResponse",
    "wisdom>DeleteQuickResponse",
    "wisdom:PutFeedback"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonConnectEnabled" : "True"
    }
  }
},
{
  "Sid" : "AllowListOperationForWisdom",
  "Effect" : "Allow",
  "Action" : [
    "wisdom:ListAssistants",
    "wisdom:ListKnowledgeBases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
  "Effect" : "Allow",
  "Action" : [
    "profile:GetCalculatedAttributeForProfile",
    "profile:CreateCalculatedAttributeDefinition",
    "profile>DeleteCalculatedAttributeDefinition",
    "profile:GetCalculatedAttributeDefinition",
    "profile:UpdateCalculatedAttributeDefinition"
  ],
  "Resource" : [

```

```

    "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
  ]
},
{
  "Sid" : "AllowPutMetricsForConnectNamespace",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Connect"
    }
  }
},
{
  "Sid" : "AllowSMSVoiceOperationsForConnect",
  "Effect" : "Allow",
  "Action" : [
    "sms-voice:SendTextMessage",
    "sms-voice:DescribePhoneNumbers"
  ],
  "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy est une [politique AWS gérée](#) qui permet à Amazon Connect de synchroniser les AWS ressources entre les régions en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 27 octobre 2023, 22:38 UTC
- Heure modifiée : 27 octobre 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect>DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect>DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",

```

```
"connect:CreateAgentStatus",
"connect:UpdateAgentStatus",
"connect:DescribeAgentStatus",
"connect:ListAgentStatuses",
"connect:CreateQuickConnect",
"connect:UpdateQuickConnect*",
"connect>DeleteQuickConnect",
"connect:DescribeQuickConnect",
"connect:ListQuickConnects",
"connect:CreateHoursOfOperation",
"connect:UpdateHoursOfOperation",
"connect>DeleteHoursOfOperation",
"connect:DescribeHoursOfOperation",
"connect:ListHoursOfOperations",
"connect:CreateQueue",
"connect:UpdateQueue*",
"connect>DeleteQueue",
"connect:DescribeQueue",
"connect:ListQueue*",
"connect:CreatePrompt",
"connect:UpdatePrompt",
"connect>DeletePrompt",
"connect:DescribePrompt",
"connect:ListPrompts",
"connect:GetPromptFile",
"connect:CreateSecurityProfile",
"connect:UpdateSecurityProfile",
"connect>DeleteSecurityProfile",
"connect:DescribeSecurityProfile",
"connect:ListSecurityProfile*",
"connect:CreateContactFlow*",
"connect:UpdateContactFlow*",
"connect>DeleteContactFlow*",
"connect:DescribeContactFlow*",
"connect:ListContactFlow*",
"connect:BatchGetFlowAssociation",
"connect:CreatePredefinedAttribute",
"connect:UpdatePredefinedAttribute",
"connect>DeletePredefinedAttribute",
"connect:DescribePredefinedAttribute",
"connect:ListPredefinedAttributes",
"connect:ListTagsForResource",
"connect:TagResource",
"connect:UntagResource",
```

```

    "connect:ListTrafficDistributionGroups",
    "connect:ListPhoneNumbersV2",
    "connect:UpdatePhoneNumber",
    "connect:DescribePhoneNumber",
    "connect:Associate*",
    "connect:Disassociate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPutMetricsForConnectNamespace",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Connect"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonConnectVoiceIDFullAccess

AmazonConnectVoiceIDFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon Connect Voice ID

Utilisation de cette stratégie

Vous pouvez AmazonConnectVoiceIDFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 26 septembre 2021, 19:04 UTC
- Heure modifiée : 26 septembre 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDataZoneDomainExecutionRolePolicy

AmazonDataZoneDomainExecutionRolePolicy est une [politique AWS gérée](#) qui : Politique par défaut pour le rôle DataZone de DomainExecutionRole service d'Amazon. Ce rôle est utilisé par

Amazon DataZone pour cataloguer, découvrir, gérer, partager et analyser les données du DataZone domaine Amazon.

Utilisation de cette politique

Vous pouvez vous associer `AmazonDataZoneDomainExecutionRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 27 septembre 2023, 21:55 UTC
- Heure modifiée : 12 mars 2024, 23h48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
```

```
"datazone:CreateEnvironment",
"datazone:CreateEnvironmentBlueprint",
"datazone:CreateEnvironmentProfile",
"datazone:CreateFormType",
"datazone:CreateGlossary",
"datazone:CreateGlossaryTerm",
"datazone:CreateListingChangeSet",
"datazone:CreateProject",
"datazone:CreateProjectMembership",
"datazone:CreateSubscriptionGrant",
"datazone:CreateSubscriptionRequest",
"datazone>DeleteAsset",
"datazone>DeleteAssetType",
"datazone>DeleteDataSource",
"datazone>DeleteEnvironment",
"datazone>DeleteEnvironmentBlueprint",
"datazone>DeleteEnvironmentProfile",
"datazone>DeleteFormType",
"datazone>DeleteGlossary",
"datazone>DeleteGlossaryTerm",
"datazone>DeleteListing",
"datazone>DeleteProject",
"datazone>DeleteProjectMembership",
"datazone>DeleteSubscriptionGrant",
"datazone>DeleteSubscriptionRequest",
"datazone>DeleteSubscriptionTarget",
"datazone:GetAsset",
"datazone:GetAssetType",
"datazone:GetDataSource",
"datazone:GetDataSourceRun",
"datazone:GetDomain",
"datazone:GetEnvironment",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentBlueprint",
"datazone:GetEnvironmentCredentials",
"datazone:GetEnvironmentProfile",
"datazone:GetFormType",
"datazone:GetGlossary",
"datazone:GetGlossaryTerm",
"datazone:GetGroupProfile",
"datazone:GetListing",
"datazone:GetProject",
"datazone:GetSubscription",
"datazone:GetSubscriptionEligibility",
```

```
"datazone:GetSubscriptionGrant",
"datazone:GetSubscriptionRequestDetails",
"datazone:GetSubscriptionTarget",
"datazone:GetUserProfile",
"datazone:ListAccountEnvironments",
"datazone:ListAssetRevisions",
"datazone:ListDataSourceRunActivities",
"datazone:ListDataSourceRuns",
"datazone:ListDataSources",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:ListEnvironmentBlueprintConfigurationSummaries",
"datazone:ListEnvironmentBlueprints",
"datazone:ListEnvironmentProfiles",
"datazone:ListEnvironments",
"datazone:ListGroupsForUser",
"datazone:ListNotifications",
"datazone:ListProjectMemberships",
"datazone:ListProjects",
"datazone:ListSubscriptionGrants",
"datazone:ListSubscriptionRequests",
"datazone:ListSubscriptionTargets",
"datazone:ListSubscriptions",
"datazone:ListWarehouseMetadata",
"datazone:RejectPredictions",
"datazone:RejectSubscriptionRequest",
"datazone:RevokeSubscription",
"datazone:Search",
"datazone:SearchGroupProfiles",
"datazone:SearchListings",
"datazone:SearchTypes",
"datazone:SearchUserProfiles",
"datazone:StartDataSourceRun",
"datazone:UpdateDataSource",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentBlueprint",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:UpdateEnvironmentProfile",
"datazone:UpdateGlossary",
"datazone:UpdateGlossaryTerm",
"datazone:UpdateProject",
"datazone:UpdateSubscriptionGrantStatus",
"datazone:UpdateSubscriptionRequest",
"datazone:StartMetadataGenerationRun",
"datazone:GetMetadataGenerationRun",
```

```
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RAMResourceShareStatement",
    "Effect" : "Allow",
    "Action" : "ram:GetResourceShareAssociations",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

AmazonDataZoneEnvironmentRolePermissionsBoundary est une [politique AWS gérée](#) qui : Amazon DataZone crée des rôles IAM pour les environnements afin d'effectuer des actions d'analyse de données, et utilise cette politique lors de la création de ces rôles pour définir les limites de leurs autorisations.

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneEnvironmentRolePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 septembre 2023, 23:38 UTC
- Heure modifiée : 17 novembre 2023, 23h29 UTC

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

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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

```

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

```

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



```
"athena:BatchGetPreparedStatement",
"athena:BatchGetQueryExecution",
"athena:CreateNamedQuery",
"athena:CreateNotebook",
"athena:CreatePreparedStatement",
"athena:CreatePresignedNotebookUrl",
"athena>DeleteNamedQuery",
"athena>DeleteNotebook",
"athena>DeletePreparedStatement",
"athena:ExportNotebook",
"athena:GetDatabase",
"athena:GetDataCatalog",
"athena:GetNamedQuery",
"athena:GetPreparedStatement",
"athena:GetQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryRuntimeStatistics",
"athena:GetTableMetadata",
"athena:GetWorkGroup",
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatement",
"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:ListPreparedStatement",
"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" : [
    "*"
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZoneFullAccess

AmazonDataZoneFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon DataZone via un accès limité aux services connexes requis par celui-ci. AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 20:06 UTC
- Heure modifiée : 12 mars 2024, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AmazonDataZoneStatement",
    "Effect" : "Allow",
    "Action" : [
      "datazone:*"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "ReadOnlyStatement",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
      "iam:ListRoles",
      "sso:DescribeRegisteredRegions",
      "s3:ListAllMyBuckets",
      "redshift:DescribeClusters",
      "redshift-serverless:ListWorkgroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "secretsmanager:ListSecrets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "BucketReadOnlyStatement",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Sid" : "CreateBucketStatement",
    "Effect" : "Allow",
    "Action" : "s3:CreateBucket",
```

```
    "Resource" : "arn:aws:s3:::amazon-datazone*"
  },
  {
    "Sid" : "RamCreateResourceStatement",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "ram:RequestedResourceType" : "datazone:Domain"
      }
    }
  },
  {
    "Sid" : "RamResourceStatement",
    "Effect" : "Allow",
    "Action" : [
      "ram>DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:RejectResourceShareInvitation"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : [
          "DataZone*"
        ]
      }
    }
  },
  {
    "Sid" : "RamResourceReadOnlyStatement",
    "Effect" : "Allow",
    "Action" : [
      "ram:GetResourceShares",
      "ram:GetResourceShareInvitations",
      "ram:GetResourceShareAssociations"
    ],
    "Resource" : "*"
  },
  {
```

```

    "Sid" : "IAMPassRoleStatement",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/AmazonDataZone*",
      "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:passedToService" : "datazone.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DataZoneTagOnCreate",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:AmazonDataZone-*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AmazonDataZoneDomain"
        ]
      },
      "StringLike" : {
        "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
        "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*"
      },
      "Null" : {
        "aws:TagKeys" : "false"
      }
    }
  },
  {
    "Sid" : "CreateSecretStatement",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:AmazonDataZone-*",
    "Condition" : {
      "StringLike" : {

```

```
        "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZoneFullUserAccess

AmazonDataZoneFullUserAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon DataZone, mais n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés.

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneFullUserAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 21:06 UTC
- Heure modifiée : 12 mars 2024, 23h47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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



```

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

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZoneGlueManageAccessRolePolicy

AmazonDataZoneGlueManageAccessRolePolicy est une [politique AWS gérée](#) qui : La politique accorde des autorisations permettant DataZone à Amazon d'activer les autorisations de publication et d'accès aux données.

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneGlueManageAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 22 septembre 2023, 20:21 UTC
- Heure modifiée : 14 décembre 2023, 23h03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTableDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:GetDatabases",
```

```

    "glue:GetTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "LakeformationResourceSharingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation>DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CrossAccountRAMResourceSharingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue>DeleteResourcePolicy",
    "glue:PutResourcePolicy"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",

```

```
    "arn:aws:glue:*:*:table/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "ram.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "ram:RequestedResourceType" : [
        "glue:Table",
        "glue:Database",
        "glue:Catalog"
      ]
    }
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "lakeformation.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ram:AssociateResourceShare",
    "ram>DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram:ListResourceSharePermissions",
    "ram:UpdateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:ResourceShareName" : [
        "LakeFormation*"
      ]
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "lakeformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
  "Effect" : "Allow",
  "Action" : "ram:AssociateResourceSharePermission",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "lakeformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSDecryptPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt"
  ],
  "Resource" : "*"
}

```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/datazone:projectId" : "proj-all"
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy est une [politique AWS gérée](#) qui : Fournit un accès complet aux DataZone API Amazon

Utilisation de cette stratégie

Vous pouvez les associer AmazonDataZonePortalFullAccessPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 mars 2023, 18:24 UTC
- Heure modifiée : 26 mars 2023, 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess est un [AWS politique gérée](#) qui : fournit un accès complet à la version préliminaire d'AmazonDataZone via le AWS Management Console. Fournit également un accès sélectif à d'autres services connexes.

Utilisation de cette politique

Vous pouvez joindre AmazonDataZonePreviewConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée

- Heure de création: 28 mars 2023, 15h16 UTC
- Heure de modification :13 juillet 2023, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

Version de la politique

Version de la politique : v2(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

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



```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateConnection"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:connection/AmazonDataZone-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:GetPolicy",
    "Resource" : [
      "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-AmazonDataZoneBootstrapRole",
      "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneServicePolicy-AmazonDataZoneServiceRole"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/AmazonDataZoneServiceRole*",
      "arn:aws:iam:*:*:role/service-role/AmazonDataZoneServiceRole*",
      "arn:aws:iam:*:*:role/AmazonDataZoneBootstrapRole*",
      "arn:aws:iam:*:*:role/service-role/AmazonDataZoneBootstrapRole",
      "arn:aws:iam:*:*:role/AmazonDataZoneDomainExecutionRole",
      "arn:aws:iam:*:*:role/service-role/AmazonDataZoneDomainExecutionRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:passedToService" : "datazonecontrol.amazonaws.com"
      }
    }
  }
}

```

```
    }  
  }  
]  
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary est une [politique AWS gérée](#) qui : Amazon DataZone crée des rôles IAM qu'il utilise pour déployer des projets d'analyse de données. DataZone utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

Utilisation de cette stratégie

Vous pouvez AmazonDataZoneProjectDeploymentPermissionsBoundary les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 mars 2023, 02:54 UTC
- Heure modifiée : 4 avril 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

```

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

```

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

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

```

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

```

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



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

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

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDataZoneProjectRolePermissionsBoundary

AmazonDataZoneProjectRolePermissionsBoundaryest une [politiqueAWS gérée](#) qui : Amazon DataZone crée des rôles IAM pour les projets afin d'effectuer des actions d'analyse de données, et utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

Utilisation de cette stratégie

Vous pouvezAmazonDataZoneProjectRolePermissionsBoundary les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 mars 2023, 02:51 UTC
- Heure modifiée : 21 mars 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

```

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

```

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

```

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



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

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicy est une [politique AWS gérée](#) qui : Amazon DataZone est un service de gestion des données qui vous permet de cataloguer, de découvrir, de gouverner, de partager et d'analyser vos données. Avec Amazon DataZone, vous pouvez partager et accéder à vos données entre différents comptes et régions prises en charge. Amazon DataZone simplifie votre expérience sur l'ensemble AWS des services, y compris, mais sans s'y limiter, Amazon Redshift, Amazon Athena AWS , Glue et AWS Lake Formation.

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneRedshiftGlueProvisioningPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 20:19 UTC
- Heure modifiée : 12 mars 2024, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

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

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

```
    ]
  }
}
},
{
  "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:DeleteDatabase"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena:DeleteWorkGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
  "Effect" : "Allow",
  "Action" : [
    "athena:CreateWorkGroup",
    "athena:TagResource",
    "iam:TagRole",
    "iam:TagPolicy",
    "logs:TagLogGroup"
  ],
}
```

```
"Resource" : "*",
"Condition" : {
  "ForAnyValue:StringLike" : {
    "aws:TagKeys" : "AmazonDataZoneEnvironment"
  },
  "Null" : {
    "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
  },
  "StringEquals" : {
    "aws:CalledViaFirst" : [
      "cloudformation.amazonaws.com"
    ]
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : "AmazonDataZoneEnvironment"
    },
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    },
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
  "Action" : [
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
  "Effect" : "Allow",
```



```
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    },
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeletePolicy",
      "iam:CreatePolicy",
      "iam:GetPolicy",
      "iam:ListPolicyVersions"
    ],
    "Resource" : [
      "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:ListBucket"
    ],
    "Resource" : "arn:aws:s3::*:*"
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
  },
```

```

    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
    "Effect" : "Allow",
    "Action" : [
      "glue:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "AmazonDataZoneEnvironment"
      },
      "Null" : {
        "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "RedshiftDataPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift-data:ListSchemas",

```

```
    "redshift-data:ExecuteStatement"
  ],
  "Resource" : [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "DescribeStatementPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:DescribeStatement"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetSecretValuePermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

AmazonDataZoneRedshiftManageAccessRolePolicy est une [politique AWS gérée](#) qui : Cette politique autorise Amazon à DataZone publier les données Amazon Redshift dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées dans le catalogue Amazon Redshift ou Amazon Redshift Serverless.

Utilisation de cette politique

Vous pouvez vous associer AmazonDataZoneRedshiftManageAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 22 septembre 2023, 20:15 UTC
- Heure modifiée : 16 novembre 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
```

```

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

```

```

    }
  },
  {
    "Sid" : "redshiftDataPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift-data:DescribeStatement",
      "redshift-data:GetStatementResult",
      "redshift:DescribeClusters"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "dataSharesPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:AuthorizeDataShare",
      "redshift:DescribeDataShares"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:datashare:*/datazone*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "associateDataShareConsumerPermission",
    "Effect" : "Allow",
    "Action" : "redshift:AssociateDataShareConsumer",
    "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDetectiveFullAccess

AmazonDetectiveFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console

Utilisation de cette stratégie

Vous pouvez AmazonDetectiveFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails de politiques

- Type : politique AWS gérée
- Heure de création : 30 avril 2020, 17:57 UTC
- Heure modifiée : 17 mai 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "guardduty:ArchiveFindings"
    ],
    "Resource" : "arn:aws:guardduty:*:*:detector/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "guardduty:GetFindings",
      "guardduty:ListDetectors"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "securityHub:GetFindings"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDetectiveInvestigatorAccess

AmazonDetectiveInvestigatorAccess est une [politique AWS gérée](#) qui : fournit aux enquêteurs un accès au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console. Cette politique accorde l'autorisation de plonger dans Detective à des fins d'enquête et un accès écrit limité à Guardduty.

Utilisation de cette politique

Vous pouvez vous associer `AmazonDetectiveInvestigatorAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 janvier 2023, 15:24 UTC
- Heure modifiée : 27 novembre 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
      ]
    }
  ]
}
```

```
    "detective:ListInvitations",
    "detective:ListMembers",
    "detective:ListOrganizationAdminAccount",
    "detective:ListTagsForResource",
    "detective:SearchGraph",
    "detective:StartInvestigation",
    "detective:GetInvestigation",
    "detective:ListInvestigations",
    "detective:UpdateInvestigationState",
    "detective:ListIndicators",
    "detective:InvokeAssistant"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GuardDutyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "guardduty:ArchiveFindings",
    "guardduty:GetFindings",
    "guardduty:ListDetectors"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecurityHubPermissions",
  "Effect" : "Allow",
  "Action" : [
    "securityHub:GetFindings"
  ],
  "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonDetectiveMemberAccess

AmazonDetectiveMemberAccess est une [politique AWS gérée](#) qui : fournit aux membres un accès au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console.

Utilisation de cette stratégie

Vous pouvez AmazonDetectiveMemberAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 janvier 2023, 15:16 UTC
- Heure modifiée : 17 janvier 2023, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "detective:AcceptInvitation",
    "detective:BatchGetMembershipDatasources",
    "detective:DisassociateMembership",
    "detective:GetFreeTrialEligibility",
    "detective:GetPricingInformation",
    "detective:GetUsageInformation",
    "detective:ListInvitations",
    "detective:RejectInvitation"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess est une [politiqueAWS gérée](#) qui : fournit aux Organizations un accès à la gestion de l'administrateur délégué pour Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console. Cela accorde l'autorisation de créer un rôle lié à un service pour Detective.

Utilisation de cette stratégie

Vous pouvez AmazonDetectiveOrganizationsAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 2 mars 2023, 15:20 UTC
- Heure modifiée : 2 mars 2023, 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "detective.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "detective.amazonaws.com",
        "guardduty.amazonaws.com",
        "macie.amazonaws.com",
        "securityhub.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDetectiveServiceLinkedRolePolicy

AmazonDetectiveServiceLinkedRolePolicyest une [politiqueAWS gérée](#) qui : Permet à Amazon Detective de passer des appels de service en votre nom

des politiques de politique de stratégie politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les politiques politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 18 novembre 2021, 19:47 UTC
- Heure modifiée : 18 novembre 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut d'une politique est la version qui définit les autorisations pour la politique qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers vers les autorisations de moindre privilège avec politiques gérées et évoluez vers vers vers les autorisations](#)

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess est une [politiqueAWS gérée](#) qui : La politique accorde un accès complet à la console DevOps Guru.

Utilisation de cette stratégie

Vous pouvez AmazonDevOpsGuruConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 17 décembre 2021, 18:43 UTC
- Heure modifiée : 25 août 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsTopicOperations",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:GetTopicAttributes",
      "sns:SetTopicAttributes",
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
  },
  {
    "Sid" : "DevOpsGuruSlrCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "devops-guru.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DevOpsGuruSlrDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
},

```

```
{
  "Sid" : "PerformanceInsightsMetricsDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "pi:GetResourceMetrics",
    "pi:DescribeDimensionKeys"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchLogsFilterLogEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:FilterLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon DevOps Guru.

Utilisation de cette stratégie

Vous pouvez AmazonDevOpsGuruFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2020, 16:38 UTC
- Heure modifiée : 25 août 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
```

```

    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsListTopicsAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsTopicOperations",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:GetTopicAttributes",
      "sns:SetTopicAttributes",
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
  },
  {
    "Sid" : "DevOpsGuruSlrCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "devops-guru.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DevOpsGuruSlrDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],

```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsFilterLogEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs::*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess est une [politique AWS gérée](#) qui : fournit un accès pour activer et gérer Amazon DevOps Guru au sein d'une organisation.

Utilisation de cette stratégie

Vous pouvez `AmazonDevOpsGuruOrganizationsAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 novembre 2021, 23:50 UTC
- Heure modifiée : 15 novembre 2021, 23 h 50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
```

```

    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListAccounts",
      "organizations:ListChildren",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListRoots"
    ],
    "Resource" : "arn:aws:organizations::*:*"
  },
  {
    "Sid" : "OrganizationsAdminDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DeregisterDelegatedAdministrator",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "devops-guru.amazonaws.com"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à la console Amazon DevOps Guru.

Utilisation de cette stratégie

Vous pouvez les associer AmazonDevOpsGuruReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 décembre 2020, 16:34 UTC
- Heure modifiée : 25 août 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
```

```

    "devops-guru:DescribeResourceCollectionHealth",
    "devops-guru:DescribeServiceIntegration",
    "devops-guru:GetCostEstimation",
    "devops-guru:GetResourceCollection",
    "devops-guru:ListAnomaliesForInsight",
    "devops-guru:ListEvents",
    "devops-guru:ListInsights",
    "devops-guru:ListAnomalousLogGroups",
    "devops-guru:ListMonitoredResources",
    "devops-guru:ListNotificationChannels",
    "devops-guru:ListRecommendations",
    "devops-guru:SearchInsights",
    "devops-guru:StartCostEstimation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudFormationListStacksAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
},
{
  "Sid" : "CloudWatchGetMetricDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RDSDescribeDBInstancesAccess",
  "Effect" : "Allow",

```

```
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsFilterLogEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy est une [politique AWS gérée](#) qui : Un rôle lié à un service est requis pour qu'Amazon DevOpsGuru puisse accéder à vos ressources.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 1 décembre 2020, 10:24 UTC
- Heure modifiée : 10 janvier 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Version de la politique

Version de la politique :v9 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",

```

```
"config:DescribeConfigurationRecorderStatus",
"config:GetResourceConfigHistory",
"events:ListRuleNamesByTarget",
"xray:GetServiceGraph",
"organizations:ListRoots",
"organizations:ListChildren",
"organizations:ListDelegatedAdministrators",
"pi:GetResourceMetrics",
"tag:GetResources",
"lambda:GetFunction",
"lambda:GetFunctionConcurrency",
"lambda:GetAccountSettings",
"lambda:ListProvisionedConcurrencyConfigs",
"lambda:ListAliases",
"lambda:ListEventSourceMappings",
"lambda:GetPolicy",
"ec2:DescribeSubnets",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"sqs:GetQueueAttributes",
"kinesis:DescribeStream",
"kinesis:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeLimits",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeStream",
"dynamodb:ListStreams",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"rds:DescribeDBInstances",
"rds:DescribeDBClusters",
"rds:DescribeOptionGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeAccountAttributes",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"s3:GetBucketNotification",
"s3:GetBucketPolicy",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketTagging",
"s3:GetBucketWebsite",
"s3:GetIntelligentTieringConfiguration",
"s3:GetLifecycleConfiguration",
```

```
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPutTargetsOnASpecificRule",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
},
{
  "Sid" : "AllowCreateOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsItem"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowAddTagsToOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:opsitem/*"
},
{
  "Sid" : "AllowAccessOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetOpsItem",
    "ssm:UpdateOpsItem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
```

```
        "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
    }
}
},
{
    "Sid" : "AllowCreateManagedRule",
    "Effect" : "Allow",
    "Action" : "events:PutRule",
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
},
{
    "Sid" : "AllowAccessManagedRule",
    "Effect" : "Allow",
    "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
},
{
    "Sid" : "AllowOtherOperationsOnManagedRule",
    "Effect" : "Allow",
    "Action" : [
        "events>DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition" : {
        "StringEquals" : {
            "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowTagBasedFilterLogEvents",
    "Effect" : "Allow",
    "Action" : [
        "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
    }
  },
  {
    "Sid" : "AllowAPIGatewayGetIntegrations",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*::/restapis/????????????",
      "arn:aws:apigateway:*::/restapis/*/resources",
      "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer AWS vers les autorisations de moindre privilège](#)

AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole est une [politique AWS gérée](#) qui : donne accès au téléchargement des journaux de réplication DMS vers les journaux Cloudwatch depuis le compte client.

Utilisation de cette stratégie

Vous pouvez AmazonDMSCloudWatchLogsRole l'associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique relative aux rôles de service
- Heure de création : 07 janvier 2016, 23:44 UTC
- Heure modifiée : 23 mai 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Sid" : "AllowCreationOfDmsLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ]
  },
  {
    "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDMSRedshiftS3Role

AmazonDMSRedshiftS3Role est une [politique AWS gérée](#) qui : Permet d'accéder à la gestion des paramètres S3 pour les points de terminaison Redshift pour DMS.

Utilisation de cette stratégie

Vous pouvez `AmazonDMSRedshiftS3Role` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2016, 17:05 UTC
- Heure modifiée : 8 juillet 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
```

```
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::dms-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole est une [politique AWS gérée](#) qui : Fournit l'accès à la gestion des paramètres VPC pour les configurations client AWS gérées

Utilisation de cette stratégie

Vous pouvez AmazonDMSVPCManagementRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 18 novembre 2015, 16:33 UTC
- Heure modifiée : 23 mai 2016, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDocDB-ElasticServiceRolePolicy

AmazonDocDB-ElasticServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à Amazon DocumentDB-Elastic de gérer AWS des ressources en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Obtenir les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 30 novembre 2022, 14:17 UTC
- Heure modifiée : 30 novembre 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDocDBConsoleFullAccess

AmazonDocDBConsoleFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à la gestion d'Amazon DocumentDB avec la compatibilité MongoDB à l'aide duAWS Management Console. Notez que cette politique accorde également un accès complet à toutes les rubriques SNS du compte, des autorisations pour créer et modifier des instances Amazon EC2 et des configurations VPC, des autorisations pour afficher et répertorier les clés sur Amazon KMS, ainsi qu'un accès complet à Amazon RDS et Amazon Neptune.

Utilisation de cette stratégie

Vous pouvez les associerAmazonDocDBConsoleFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 janvier 2019, 20:37 UTC
- Heure modifiée : 30 novembre 2022, 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic>DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic>DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds>DeleteDBCluster",
        "rds>DeleteDBClusterParameterGroup",
        "rds>DeleteDBClusterSnapshot",
        "rds>DeleteDBInstance",
        "rds>DeleteDBParameterGroup",
        "rds>DeleteDBSubnetGroup",
        "rds>DeleteEventSubscription",
```



```
"rds:DeleteGlobalCluster",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:ModifyGlobalCluster",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveFromGlobalCluster",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
"rds: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"
    }
  }
}

```

```
}
  }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDocDBElasticFullAccess

AmazonDocDBElasticFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux clusters Elastic d'Amazon DocumentDB et aux autres autorisations requises pour ses dépendances, notamment EC2SecretsManager, CloudWatch KMS et IAM.

Utilisation de cette politique

Vous pouvez l'associer AmazonDocDBElasticFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 5 juin 2023, 13:51 UTC
- Heure modifiée : 21 juin 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic>DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic>DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2>DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt",
      "kms:DescribeKey",
      "kms:GenerateDataKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "docdb-elastic.*.amazonaws.com"
        ],
        "aws:ResourceTag/DocDBElasticFullAccess" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/DocDBElasticFullAccess" : "*",
        "kms:ViaService" : [
          "docdb-elastic.*.amazonaws.com"
        ]
      }
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
}
```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AmazonDocDBElasticReadOnlyAccess

AmazonDocDBElasticReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon DocDB-Elastic et aux métriques. CloudWatch

Utilisation de cette politique

Vous pouvez l'associer AmazonDocDBElasticReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 8 juin 2023, 14:37 UTC
- Heure modifiée : 21 juin 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



```
{
  "Effect" : "Allow",
  "Action" : [
    "docdb-elastic:ListClusters",
    "docdb-elastic:GetCluster",
    "docdb-elastic:ListClusterSnapshots",
    "docdb-elastic:GetClusterSnapshot",
    "docdb-elastic:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AmazonDocDBFullAccess

AmazonDocDBFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon DocumentDB avec compatibilité MongoDB. Notez que cette politique accorde également un accès complet à la publication sur toutes les rubriques SNS du compte et un accès complet à Amazon RDS et Amazon Neptune.

Utilisation de cette stratégie

Vous pouvez AmazonDocDBFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 janvier 2019, 20:21 UTC
- Heure modifiée : 9 janvier 2019, 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds>DeleteDBCluster",
        "rds>DeleteDBClusterParameterGroup",
        "rds>DeleteDBClusterSnapshot",
        "rds>DeleteDBInstance",
```

```
"rds:DeleteDBParameterGroup",
"rds:DeleteDBSubnetGroup",
"rds:DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
"rds:RemoveTagsForResource",
"rds:ResetDBClusterParameterGroup",
"rds:ResetDBParameterGroup",
"rds:RestoreDBClusterFromSnapshot",
```

```

    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "rds.amazonaws.com"
    }
  }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDocDBReadOnlyAccess

AmazonDocDBReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon DocumentDB avec compatibilité MongoDB. Notez que cette politique autorise également l'accès aux ressources Amazon RDS et Amazon Neptune.

Utilisation de cette stratégie

Vous pouvez AmazonDocDBReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 janvier 2019, 20:30 UTC
- Heure modifiée : 09 janvier 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "rds:DescribeAccountAttributes",
      "rds:DescribeCertificates",
      "rds:DescribeDBClusterParameterGroups",
      "rds:DescribeDBClusterParameters",
      "rds:DescribeDBClusterSnapshotAttributes",
      "rds:DescribeDBClusterSnapshots",
      "rds:DescribeDBClusters",
      "rds:DescribeDBEngineVersions",
      "rds:DescribeDBInstances",
      "rds:DescribeDBLogFiles",
      "rds:DescribeDBParameterGroups",
      "rds:DescribeDBParameters",
      "rds:DescribeDBSubnetGroups",
      "rds:DescribeEventCategories",
      "rds:DescribeEventSubscriptions",
      "rds:DescribeEvents",
      "rds:DescribeOrderableDBInstanceOptions",
      "rds:DescribePendingMaintenanceActions",
      "rds:DownloadDBLogFilePortion",
      "rds:ListTagsForResource"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",

```

```

    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "kms:ListAliases",
    "kms:ListKeyPolicies"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDRSVPCManagement

AmazonDRSVPCManagement est une [politique AWS gérée](#) qui : fournit un accès à la gestion des paramètres VPC pour les configurations client gérées par Amazon

Utilisation de cette stratégie

Vous pouvez associer AmazonDRSVPCManagement à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 septembre 2015, 00:09 UTC
- Heure modifiée : 2 septembre 2015, 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ]
    }
  ]
}
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDynamoDBFullAccess

AmazonDynamoDBFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon DynamoDB via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonDynamoDBFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 29 janvier 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline>DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:ListSubscriptions",
```

```

    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sns:SetTopicAttributes",
    "lambda:CreateFunction",
    "lambda:ListFunctions",
    "lambda:ListEventSourceMappings",
    "lambda:CreateEventSourceMapping",
    "lambda>DeleteEventSourceMapping",
    "lambda:GetFunctionConfiguration",
    "lambda>DeleteFunction",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "resource-groups:GetGroup",
    "resource-groups:GetGroupQuery",
    "resource-groups>DeleteGroup",
    "resource-groups:CreateGroup",
    "tag:GetResources",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:DescribeStreamSummary"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "cloudwatch:GetInsightRuleReport",
  "Effect" : "Allow",
  "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "application-autoscaling.amazonaws.com",
        "application-autoscaling.amazonaws.com.cn",
        "dax.amazonaws.com"
      ]
    }
  }
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "replication.dynamodb.amazonaws.com",
        "dax.amazonaws.com",
        "dynamodb.application-autoscaling.amazonaws.com",
        "contributorinsights.dynamodb.amazonaws.com",
        "kinesisreplication.dynamodb.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDynamoDBFullAccesswithDataPipeline

AmazonDynamoDBFullAccesswithDataPipeline est une [politique AWS gérée](#) qui : Cette politique est en voie d'obsolescence. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>. Fournit un accès complet à Amazon DynamoDB, y compris l'exportation/importation à l'aide du AWS Data Pipeline via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez `AmazonDynamoDBFullAccesswithDataPipeline` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 12 novembre 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
```

```
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sns:SetTopicAttributes"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsole"
},
{
  "Action" : [
    "lambda:*",
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsoleTriggers"
},
{
  "Action" : [
    "datapipeline:*",
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsoleImportExport"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRolePolicy",
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Sid" : "IAMEDPRoles"
},
{
  "Action" : [
    "ec2:CreateTags",
    "ec2:DescribeInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
```

```
    "ec2:TerminateInstances",
    "elasticmapreduce:*",
    "datapipeline:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "EMR"
},
{
  "Action" : [
    "s3:DeleteObject",
    "s3:Get*",
    "s3:List*",
    "s3:Put*"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Sid" : "S3"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonDynamoDBReadOnlyAccess

AmazonDynamoDBReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon DynamoDB via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonDynamoDBReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 20 mars 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",

```



```

    "dynamodb:GetItem",
    "dynamodb:GetResourcePolicy",
    "dynamodb:Query",
    "dynamodb:Scan",
    "dynamodb: PartiQLSelect",
    "dax:Describe*",
    "dax:List*",
    "dax:GetItem",
    "dax:BatchGetItem",
    "dax:Query",
    "dax:Scan",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "lambda:ListFunctions",
    "lambda:ListEventSourceMappings",
    "lambda:GetFunctionConfiguration",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "resource-groups:GetGroup",
    "resource-groups:GetGroupQuery",
    "tag:GetResources",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:DescribeStreamSummary"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "CCIAccess",
  "Action" : "cloudwatch:GetInsightRuleReport",
  "Effect" : "Allow",
  "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy est une [politique AWS gérée](#) qui : politique IAM qui autorise le compte de pilote CSI à effectuer des appels aux services connexes tels que EC2 en votre nom.

Utilisation de cette politique

Vous pouvez les associer AmazonEBSCSIDriverPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 4 avril 2022, 17:24 UTC
- Heure modifiée : 18 novembre 2022, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:ModifyVolume",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTags",
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumesModifications"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateVolume",
        "CreateSnapshot"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/CSIVolumeName" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
```

```
        "ec2:ResourceTag/CSIVolumeName" : "*"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteVolume"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteSnapshot"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteSnapshot"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerRegistryFullAccess

AmazonEC2ContainerRegistryFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès administratif aux ressources Amazon ECR

Utilisation de cette stratégie

Vous pouvez AmazonEC2ContainerRegistryFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 décembre 2015, 17:06 UTC
- Heure modifiée : 5 décembre 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:*",
      "cloudtrail:LookupEvents"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "replication.ecr.amazonaws.com"
        ]
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerRegistryPowerUser

AmazonEC2ContainerRegistryPowerUser est une [politiqueAWS gérée](#) qui : fournit un accès complet aux référentiels Amazon EC2 Container Registry, mais n'autorise pas la suppression de référentiels ni la modification des politiques.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonEC2ContainerRegistryPowerUser` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 décembre 2015, 17:05 UTC
- Heure modifiée : 10 décembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",

```



```
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerRegistryReadOnly

AmazonEC2ContainerRegistryReadOnly est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule aux référentiels Amazon EC2 Container Registry.

Utilisation de cette stratégie

Vous pouvez AmazonEC2ContainerRegistryReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 décembre 2015, 17:04 UTC
- Heure modifiée : 10 décembre 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole est une [politique AWS gérée qui : Politique](#) visant à activer l'autodimensionnement des tâches pour Amazon EC2 Container Service

Utilisation de cette stratégie

Vous pouvez AmazonEC2ContainerServiceAutoscaleRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 12 mai 2016, 23:25 UTC
- Heure modifiée : 5 février 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ]
    }
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerServiceEventsRole

AmazonEC2ContainerServiceEventsRole est une [politiqueAWS gérée](#) qui : Politique d'activation CloudWatch des événements pour EC2 Container Service

Utilisation de cette stratégie

Vous pouvez AmazonEC2ContainerServiceEventsRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 30 mai 2017, 16:51 UTC

- Heure modifiée : 6 mars 2023, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "RunTask"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerServiceforEC2Role

AmazonEC2ContainerServiceforEC2Role est une [politique AWS gérée](#) qui : Politique par défaut pour le rôle Amazon EC2 pour Amazon EC2 Container Service.

Utilisation de cette stratégie

Vous pouvez AmazonEC2ContainerServiceforEC2Role les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 mars 2015, 18:45 UTC
- Heure modifiée : 6 mars 2023, 22:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ContainerServiceRole

AmazonEC2ContainerServiceRole est une [politiqueAWS gérée qui : Politique](#) par défaut pour le rôle de service Amazon ECS.

Utilisation de cette stratégie

Vous pouvez les associer AmazonEC2ContainerServiceRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 avril 2015, 16:14 UTC
- Heure modifiée : 11 août 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2FullAccess

AmazonEC2FullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon EC2 via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonEC2FullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : "autoscaling:*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "autoscaling.amazonaws.com",
        "ec2scheduled.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "transitgateway.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon EC2 via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonEC2ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 14 février 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
```

```
    "Effect" : "Allow",
    "Action" : "autoscaling:Describe*",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy est une [politique AWS gérée](#) qui : fournit un accès EC2 au compartiment S3 pour télécharger les révisions. Ce rôle est nécessaire à l' CodeDeploy agent sur des instances EC2.

Utilisation de cette stratégie

Vous pouvez les associer AmazonEC2RoleforAWSCodeDeploy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 mai 2015, 18:10 UTC
- Heure modifiée : 20 mars 2017, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2RoleforAWSCodeDeployLimited

AmazonEC2RoleforAWSCodeDeployLimited est une [politique AWS gérée](#) qui : fournit à EC2 un accès limité au compartiment S3 pour télécharger les révisions. L' CodeDeploy agent a besoin de ce rôle sur des instances EC2.

Utilisation de cette stratégie

Vous pouvez AmazonEC2RoleforAWSCodeDeployLimited les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 24 août 2020, 17:55 UTC
- Heure modifiée : 20 janvier 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole est une [politique AWS gérée qui : Politique](#) par défaut pour le rôle de service Amazon EC2 Role for Data Pipeline.

Utilisation de cette stratégie

Vous pouvez AmazonEC2RoleforDataPipelineRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 22 février 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2RoleforSSM

AmazonEC2RoleforSSM est une [politique AWS gérée](#) qui : Cette politique sera bientôt obsolète. À la place, utilisez la ManagedInstanceCore politique AmazonSSM pour activer la fonctionnalité principale du service AWS Systems Manager sur les instances EC2. Pour plus d'informations, consultez <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

Utilisation de cette politique

Vous pouvez AmazonEC2RoleforSSM les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 29 mai 2015, 17:48 UTC
- Heure modifiée : 24 janvier 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
```

```

    "ssm:GetParameters",
    "ssm:ListAssociations",
    "ssm:ListInstanceAssociations",
    "ssm:PutInventory",
    "ssm:PutComplianceItems",
    "ssm:PutConfigurePackageResult",
    "ssm:UpdateAssociationStatus",
    "ssm:UpdateInstanceAssociationStatus",
    "ssm:UpdateInstanceInformation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2messages:AcknowledgeMessage",
    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [

```

```
    "ec2:DescribeInstanceStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",
    "ds:DescribeDirectories"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetEncryptionConfiguration",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2RolePolicyForLaunchWizard

AmazonEC2RolePolicyForLaunchWizard est une [politiqueAWS gérée](#) qui : Politique gérée pour le rôle LaunchWizard de service Amazon pour EC2

Utilisation de cette stratégie

Vous pouvez AmazonEC2RolePolicyForLaunchWizard les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 novembre 2019, 08:05 UTC
- Heure modifiée : 16 mai 2022, 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
```

```

    "ec2:RebootInstances",
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReplaceRoute"
  ],
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:DescribeRegions",
    "ec2:DescribeVolumes",
    "ec2:DescribeRouteTables",
    "ec2:ModifyInstanceAttribute",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:PutMetricData",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2:CreateVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "LaunchWizardResourceGroupID",
          "LaunchWizardApplicationType"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:PutObjectTagging",
      "s3:GetBucketLocation",
      "logs:PutLogEvents",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:*",
      "arn:aws:s3:::launchwizard*",
      "arn:aws:s3:::aws-sap-data-provider/config.properties"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:Create*",
    "Resource" : "arn:aws:logs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:Describe*",
      "cloudformation:DescribeStackResources",
      "cloudformation:SignalResource",

```

```

    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStacks"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "LaunchWizardResourceGroupID"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchGetItem",
    "dynamodb:PutItem",
    "sqs:ReceiveMessage",
    "sqs:SendMessage",
    "dynamodb:Scan",
    "s3:ListBucket",
    "dynamodb:Query",
    "dynamodb:UpdateItem",
    "dynamodb>DeleteTable",
    "dynamodb>CreateTable",
    "s3:GetObject",
    "dynamodb:DescribeTable",
    "s3:GetBucketLocation",
    "dynamodb:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:dynamodb:*:*:table/LaunchWizard*",
    "arn:aws:sqs:*:*:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/LaunchWizardApplicationType" : "*"
    }
  }
},

```



```
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:GetDocument"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems",
    "fsx:ListTagsForResource",
    "fsx:DescribeStorageVirtualMachines"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2SpotFleetAutoscaleRole

AmazonEC2SpotFleetAutoscaleRole est une [politiqueAWS gérée](#) qui : Politique visant à activer l'autoscaling pour Amazon EC2 Spot Fleet

Utilisation de cette stratégie

Vous pouvez associer `AmazonEC2SpotFleetAutoscaleRole` à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 août 2016, 18:27 UTC
- Heure modifiée : 18 février 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",

```

```
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEC2SpotFleetTaggingRole

AmazonEC2SpotFleetTaggingRole est une [politique AWS gérée](#) qui : autorise EC2 Spot Fleet à demander, résilier et étiqueter des instances Spot en votre nom.

Utilisation de cette stratégie

Vous pouvez les associer AmazonEC2SpotFleetTaggingRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 29 juin 2017, 18:19 UTC
- Heure modifiée : 23 avril 2020, 19h30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      ]
    }
  ]
}
```

```
    }
  },
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:*/*"
  ]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonECS_FullAccess

AmazonECS_FullAccess est une [politique AWS gérée](#) qui : fournit un accès administratif aux ressources Amazon ECS et active les fonctionnalités ECS via l'accès à d'autres ressources de AWS service, notamment les VPC, les groupes Auto Scaling et les CloudFormation piles.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonECS_FullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 novembre 2017, 21:36 UTC
- Heure modifiée : 04 janvier 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Version de la politique

Version de la politique : v20 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
```

```
"autoscaling:CreateLaunchConfiguration",
"autoscaling>DeleteAutoScalingGroup",
"autoscaling>DeleteLaunchConfiguration",
"autoscaling:Describe*",
"autoscaling:UpdateAutoScalingGroup",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStack*",
"cloudformation:UpdateStack",
"cloudwatch>DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricStatistics",
"cloudwatch:PutMetricAlarm",
"codedeploy:BatchGetApplicationRevisions",
"codedeploy:BatchGetApplications",
"codedeploy:BatchGetDeploymentGroups",
"codedeploy:BatchGetDeployments",
"codedeploy:ContinueDeployment",
"codedeploy>CreateApplication",
"codedeploy>CreateDeployment",
"codedeploy>CreateDeploymentGroup",
"codedeploy:GetApplication",
"codedeploy:GetApplicationRevision",
"codedeploy:GetDeployment",
"codedeploy:GetDeploymentConfig",
"codedeploy:GetDeploymentGroup",
"codedeploy:GetDeploymentTarget",
"codedeploy:ListApplicationRevisions",
"codedeploy:ListApplications",
"codedeploy:ListDeploymentConfigs",
"codedeploy:ListDeploymentGroups",
"codedeploy:ListDeployments",
"codedeploy:ListDeploymentTargets",
"codedeploy:RegisterApplicationRevision",
"codedeploy:StopDeployment",
"ec2:AssociateRouteTable",
"ec2:AttachInternetGateway",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CancelSpotFleetRequests",
"ec2>CreateInternetGateway",
"ec2>CreateLaunchTemplate",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
```

```
"ec2:CreateSubnet",
"ec2:CreateVpc",
"ec2:DeleteLaunchTemplate",
"ec2:DeleteSubnet",
"ec2:DeleteVpc",
"ec2:Describe*",
"ec2:DetachInternetGateway",
"ec2:DisassociateRouteTable",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVpcAttribute",
"ec2:RequestSpotFleet",
"ec2:RunInstances",
"ecs:*",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateRule",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing>DeleteListener",
"elasticloadbalancing>DeleteLoadBalancer",
"elasticloadbalancing>DeleteRule",
"elasticloadbalancing>DeleteTargetGroup",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"events>DeleteRule",
"events:DescribeRule",
"events:ListRuleNamesByTarget",
"events:ListTargetsByRule",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"fsx:DescribeFileSystems",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListRoles",
"lambda:ListFunctions",
"logs:CreateLogGroup",
"logs:DescribeLogGroups",
"logs:FilterLogEvents",
"route53:CreateHostedZone",
"route53>DeleteHostedZone",
```



```

    "route53:GetHealthCheck",
    "route53:GetHostedZone",
    "route53:ListHostedZonesByName",
    "servicediscovery:CreatePrivateDnsNamespace",
    "servicediscovery:CreateService",
    "servicediscovery>DeleteService",
    "servicediscovery:GetNamespace",
    "servicediscovery:GetOperation",
    "servicediscovery:GetService",
    "servicediscovery:ListNamespaces",
    "servicediscovery:ListServices",
    "servicediscovery:UpdateService",
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter",
    "ssm:GetParameters",
    "ssm:GetParametersByPath"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteInternetGateway",
    "ec2:DeleteRoute",
    "ec2:DeleteRouteTable",
    "ec2:DeleteSecurityGroup"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
    }
  }
},
},

```

```
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ecs-tasks.amazonaws.com"
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/ecsInstanceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/ecsAutoscaleRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "application-autoscaling.amazonaws.com",
        "application-autoscaling.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
```

```
"Action" : "iam:CreateServiceLinkedRole",
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "iam:AWSServiceName" : [
      "autoscaling.amazonaws.com",
      "ecs.amazonaws.com",
      "ecs.application-autoscaling.amazonaws.com",
      "spot.amazonaws.com",
      "spotfleet.amazonaws.com"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "elasticloadbalancing:CreateAction" : [
        "CreateTargetGroup",
        "CreateRule",
        "CreateListener",
        "CreateLoadBalancer"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity est une [politique AWS gérée](#) qui : fournit un accès administratif à l'autorité de certification privée, à AWS Secrets Manager et aux autres entités Services AWS nécessaires pour gérer les fonctionnalités TLS d'ECS Service Connect en votre nom.

Utilisation de cette politique

Vous pouvez vous associer AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 19 janvier 2024, 20:08 UTC
- Heure modifiée : 19 janvier 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
    }
  ]
}
```

```

"Condition" : {
  "ArnLike" : {
    "aws:RequestTag/AmazonECSCreated" : [
      "arn:aws:ecs:*:*:service/*/*",
      "arn:aws:ecs:*:*:task-set/*/*"
    ]
  },
  "StringEquals" : {
    "aws:RequestTag/AmazonECManaged" : "true",
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
},
{
  "Sid" : "TagOnCreateSecret",
  "Effect" : "Allow",
  "Action" : "secretsmanager:TagResource",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
  "Condition" : {
    "ArnLike" : {
      "aws:RequestTag/AmazonECSCreated" : [
        "arn:aws:ecs:*:*:service/*/*",
        "arn:aws:ecs:*:*:task-set/*/*"
      ]
    },
    "StringEquals" : {
      "aws:RequestTag/AmazonECManaged" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RotateTLSCertificateSecret",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:UpdateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:PutSecretValue",
    "secretsmanager>DeleteSecret",
    "secretsmanager:RotateSecret",
    "secretsmanager:UpdateSecretVersionStage"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",

```

```

    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthority",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:GetCertificate",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:DescribeCertificateAuthority"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSTagged" : "true"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSTagged" : "true",
        "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonECSInfrastructureRolePolicyForVolumes

AmazonECSInfrastructureRolePolicyForVolumes est une [politique AWS gérée](#) qui : fournit l'accès aux autres ressources de AWS service nécessaires pour gérer les volumes associés aux charges de travail ECS en votre nom.

Utilisation de cette politique

Vous pouvez vous associer AmazonECSInfrastructureRolePolicyForVolumes à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 10 janvier 2024, 22:56 UTC
- Heure modifiée : 10 janvier 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Action" : "ec2:CreateVolume",
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "ArnLike" : {
    "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
  },
  "StringEquals" : {
    "aws:RequestTag/AmazonECSManaged" : "true"
  }
}
},
{
  "Sid" : "TagOnCreateVolume",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "ArnLike" : {
      "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
    },
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVolume",
      "aws:RequestTag/AmazonECSManaged" : "true"
    }
  }
}
},
{
  "Sid" : "DescribeVolumesForLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVolumes",
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ManageEBSVolumeLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
```



```
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSTagged" : "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/AmazonECSTagged" : "arn:aws:ecs:*:*:task/*"
      },
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSTagged" : "true"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy est une [politique AWS gérée](#) qui : Politique permettant à Amazon ECS de gérer votre cluster.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 14 octobre 2017, 01:18 UTC
- Heure modifiée : 4 décembre 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:Describe*",

```

```

    "ec2:DetachNetworkInterface",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:DeregisterTargets",
    "elasticloadbalancing:Describe*",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:RegisterTargets",
    "route53:ChangeResourceRecordSets",
    "route53:CreateHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:Get*",
    "route53:List*",
    "route53:UpdateHealthCheck",
    "servicediscovery:DeregisterInstance",
    "servicediscovery:Get*",
    "servicediscovery:List*",
    "servicediscovery:RegisterInstance",
    "servicediscovery:UpdateInstanceCustomHealthStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScaling",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScalingManagement",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:SetInstanceProtection",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:PutLifecycleHook",
    "autoscaling>DeleteLifecycleHook",
    "autoscaling:CompleteLifecycleAction",
    "autoscaling:RecordLifecycleActionHeartbeat"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {

```

```
        "autoscaling:ResourceTag/AmazonECSManaged" : "false"
    }
}
},
{
  "Sid" : "AutoScalingPlanManagement",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling-plans:CreateScalingPlan",
    "autoscaling-plans>DeleteScalingPlan",
    "autoscaling-plans:DescribeScalingPlans",
    "autoscaling-plans:DescribeScalingPlanResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EventBridge",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
},
{
  "Sid" : "EventBridgeRuleManagement",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "ecs.amazonaws.com"
    }
  }
},
{
  "Sid" : "CWAlarmManagement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch>DeleteAlarms",
    "cloudwatch:DescribeAlarms",
```

```
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
},
{
  "Sid" : "ECSTagging",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "CWLogGroupManagement",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
},
{
  "Sid" : "CWLogStreamManagement",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
},
{
  "Sid" : "ExecuteCommandSessionManagement",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeSessions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ExecuteCommand",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ssm:StartSession"
  ],
  "Resource" : [
    "arn:aws:ecs:*:*:task/*",
    "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
  ]
},
{
  "Sid" : "CloudMapResourceCreation",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:CreateHttpNamespace",
    "servicediscovery:CreateService"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AmazonECSManaged"
      ]
    }
  }
},
{
  "Sid" : "CloudMapResourceTagging",
  "Effect" : "Allow",
  "Action" : "servicediscovery:TagResource",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AmazonECSManaged" : "*"
    }
  }
},
{
  "Sid" : "CloudMapResourceDeletion",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:DeleteService"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonECSManaged" : "false"
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "CloudMapResourceDiscovery",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:DiscoverInstances",
    "servicediscovery:DiscoverInstancesRevision"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy est une [politique AWS gérée](#) qui : fournit l'accès à d'autres ressources AWS de service qui sont nécessaires pour exécuter les tâches Amazon ECS

Utilisation de cette politique

Vous pouvez les associer AmazonECSTaskExecutionRolePolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 16 novembre 2017, 18:48 UTC
- Heure modifiée : 16 novembre 2017, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy est un [AWS politique gérée](#) qui : fournit un accès de gestion aux ressources EFS et un accès en lecture à EC2

Utilisation de cette politique

Vous pouvez joindre `AmazonEFSCSIDriverPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 25 juillet 2023, 20h10 UTC
- Heure de modification :25 juillet 2023, 20h10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowTagNewAccessPoints",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticfilesystem:CreateAction" : "CreateAccessPoint"
      },
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowDeleteAccessPoint",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:DeleteAccessPoint",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
      }
    }
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonEKS_CNI_Policy

AmazonEKS_CNI_Policy est une [politique AWS gérée](#) qui : Cette politique fournit au plugin Amazon VPC CNI (amazon-vpc-cni-k8s) les autorisations dont il a besoin pour modifier la configuration de l'adresse IP sur vos nœuds de travail EKS. Cet ensemble d'autorisations permet au CNI de répertorier, de décrire et de modifier les interfaces réseau élastiques en votre nom. Plus d'informations sur le plugin AWS VPC CNI sont disponibles ici : <https://github.com/aws/8s/amazon-vpc-cni-k>

Utilisation de cette politique

Vous pouvez vous associer AmazonEKS_CNI_Policy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:07 UTC
- Heure modifiée : 4 mars 2024, 20h20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonEKSClusterPolicy

AmazonEKSClusterPolicy est une [politique AWS gérée](#) qui : Cette politique fournit à Kubernetes les autorisations dont il a besoin pour gérer les ressources en votre nom. Kubernetes nécessite des `CreateTags` autorisations EC2 : pour placer des informations d'identification sur les ressources EC2, y compris, mais sans s'y limiter, les instances, les groupes de sécurité et les interfaces réseau élastiques.

Utilisation de cette stratégie

Vous pouvez `AmazonEKSClusterPolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:06 UTC
- Heure modifiée : 07 février 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"autoscaling:UpdateAutoScalingGroup",
"ec2:AttachVolume",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateRoute",
"ec2:CreateSecurityGroup",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2>DeleteRoute",
"ec2>DeleteSecurityGroup",
"ec2>DeleteVolume",
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVolumesModifications",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeAvailabilityZones",
"ec2:DetachVolume",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyVolume",
"ec2:RevokeSecurityGroupIngress",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeInternetGateways",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:AttachLoadBalancerToSubnets",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateLoadBalancerListeners",
"elasticloadbalancing:CreateLoadBalancerPolicy",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing>DeleteListener",
"elasticloadbalancing>DeleteLoadBalancer",
"elasticloadbalancing>DeleteLoadBalancerListeners",
"elasticloadbalancing>DeleteTargetGroup",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```

    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DetachLoadBalancerFromSubnets",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:ModifyLoadBalancerAttributes",
    "elasticloadbalancing:ModifyTargetGroup",
    "elasticloadbalancing:ModifyTargetGroupAttributes",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
    "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSCoordinatorServiceRolePolicy

AmazonEKSCoordinatorServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique permet à Amazon EKS de gérer les AWS ressources pour le connecteur EKS

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 septembre 2021, 20:31 UTC
- Heure modifiée : 4 septembre 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy est une [stratégie AWS gérée](#) qui : fournit l'accès à d'autres ressources de AWS service qui sont nécessaires pour exécuter les pods Amazon EKS sur AWS Fargate

Utilisation de cette politique

Vous pouvez les associer AmazonEKSFargatePodExecutionRolePolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 22 novembre 2019, 04:34 UTC

- Heure modifiée : 22 novembre 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSFargateServiceRolePolicy

AmazonEKSFargateServiceRolePolicy est [AWSune des](#) des des des des des des des des des des des des

Utilisation des des de de de de

Cette politique est attachée à un rôle lié au service qui permet à ce service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des des des

- Type : Politique de rôles liée à un service
- Heure de création : 22 novembre 2019, 04:36 UTC
- Heure modifiée : 22 novembre 2019, 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de de de de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer AWS avec les autorisations de moindre privilège](#)

AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy est une [politique AWS gérée](#) qui : Cette politique fournit des autorisations aux instances du plan de contrôle du cluster local EKS exécutées sur votre compte pour gérer les ressources en votre nom.

Utilisation de cette stratégie

Vous pouvez AmazonEKSLocalOutpostClusterPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 août 2022, 21:56 UTC
- Heure modifiée : 17 octobre 2022, 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2messages:AcknowledgeMessage",
        "ec2messages>DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/eks/*",
    "arn:aws:ecr:*:*:repository/bottlerocket-admin",
    "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
    "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
    "arn:aws:ecr:*:*:repository/kubelet-config-updater"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager>DeleteSecret"
  ],
  "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:PutLogEvents",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSLocalOutpostServiceRolePolicy

AmazonEKSLocalOutpostServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon EKS Local à appeler AWS des services en votre nom.

La politique de cette politique de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politiques politiques politiques

- Type : Politique de rôles liée à un service
- 23 août 2022, 21 août 2022, 21:53 UTC de la création de 23 août 2022 d'août 2022, 21
- Heure modifiée : 24 octobre 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

politique JSON de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
```



```

    "ec2:DescribeSubnets",
    "ec2:DescribeRouteTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribePlacementGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ]
}

```

```

    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:launch-template/*",
      "arn:aws:ec2:*:*:network-interface/*",

```

```

    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:placement-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:TerminateInstances",
    "ec2:GetConsoleOutput"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*",
        "eks*"
      ]
    }
  },
  "StringEquals" : {
    "ec2:CreateAction" : [
      "CreateNetworkInterface",
      "CreateSecurityGroup",
      "RunInstances"
    ]
  }
}

```

```

    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "kubernetes.io/cluster/*",
          "eks*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "secretsmanager:DeleteSecret",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "secretsmanager:DescribeSecret",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
  },

```

```

{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile"
  ],
  "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AmazonEKS-ControlPlaneInstanceProxy"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:ResumeSession",

```

```
    "ssm:TerminateSession"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "outposts:GetOutpost"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [politiques gérées des stratégies AWS gérées gérées des stratégies gérées gérées des politiques gérées des stratégies gérées gérées des stratégies gérées gérées des stratégies gérées gérées](#)

AmazonEKSServicePolicy

AmazonEKSServicePolicy est une [politique AWS gérée](#) qui : Cette politique permet à Amazon Elastic Container Service for Kubernetes de créer et de gérer les ressources nécessaires à l'exploitation des clusters EKS.

Utilisation de cette politique

Vous pouvez AmazonEKSServicePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:08 UTC
- Heure modifiée : 27 mai 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    }
  ],
  {
```

```
"Effect" : "Allow",
"Action" : "route53:AssociateVPCWithHostedZone",
"Resource" : "*"
},
{
"Effect" : "Allow",
"Action" : "logs:CreateLogGroup",
"Resource" : "*"
},
{
"Effect" : "Allow",
"Action" : [
"logs:CreateLogStream",
"logs:DescribeLogStreams"
],
"Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
},
{
"Effect" : "Allow",
"Action" : "logs:PutLogEvents",
"Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
},
{
"Effect" : "Allow",
"Action" : "iam:CreateServiceLinkedRole",
"Resource" : "*",
"Condition" : {
"StringLike" : {
"iam:AWSServiceName" : "eks.amazonaws.com"
}
}
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSServiceRolePolicy

AmazonEKSServiceRolePolicy est une [politique AWS gérée](#) qui : Un rôle lié à un service est requis pour qu'Amazon EKS puisse appeler AWS des services en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à Service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 février 2020, 20:10 UTC
- Heure modifiée : 27 mai 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```

    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:CreateNetworkInterfacePermission",
    "iam:ListAttachedRolePolicies",
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "ec2:ResourceTag/Name" : "eks-cluster-sg*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",

```

```

    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*"
      ],
      "aws:RequestTag/Name" : "eks-cluster-sg*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "route53:AssociateVPCWithHostedZone",
  "Resource" : "arn:aws:route53:::hostedzone/*"
},
{
  "Effect" : "Allow",
  "Action" : "logs:CreateLogGroup",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
},
{
  "Effect" : "Allow",
  "Action" : "logs:PutLogEvents",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSVPCResourceController

AmazonEKSVPCResourceController est une [politiqueAWS gérée](#) qui : [Politique](#) utilisée par le contrôleur de ressources VPC pour gérer les ENI et les adresses IP des nœuds de travail.

Utilisation de cette stratégie

Vous pouvez AmazonEKSVPCResourceController les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 12 août 2020, 00:55 UTC
- Heure modifiée : 12 août 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface",
    "ec2:DetachNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2>DeleteNetworkInterface",
    "ec2:AttachNetworkInterface",
    "ec2:UnassignPrivateIpAddresses",
    "ec2:AssignPrivateIpAddresses"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy est une [politique AWS gérée](#) qui : Cette politique permet aux nœuds de travail Amazon EKS de se connecter aux clusters Amazon EKS.

Utilisation de cette politique

Vous pouvez vous associer AmazonEKSWorkerNodePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:09 UTC

- Heure modifiée : 27 novembre 2023, 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSEKSWorkerNodePolicy

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonElasticCacheFullAccess

AmazonElasticCacheFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon ElasticCache via le AWS Management Console.

Utilisation de cette politique

Vous pouvez vous associer AmazonElasticCacheFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 28 novembre 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticCacheFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonElastiCacheReadOnlyAccess

AmazonElastiCacheReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon ElastiCache via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer AmazonElastiCacheReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticContainerRegistryPublicFullAccess

AmazonElasticContainerRegistryPublicFullAccess est une [politique AWS gérée](#) qui :
Fournit un accès administratif aux ressources publiques d'Amazon ECR

Utilisation de cette stratégie

Vous pouvez AmazonElasticContainerRegistryPublicFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 décembre 2020, 17:25 UTC
- Heure modifiée : 01 décembre 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser est une [politiqueAWS gérée](#) qui : fournit un accès complet aux référentiels publics Amazon ECR, mais n'autorise pas la suppression de référentiels ni la modification des politiques.

Utilisation de cette stratégie

Vous pouvez AmazonElasticContainerRegistryPublicPowerUser les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2020, 16:16 UTC

- Heure modifiée : 01 décembre 2020, 16:16 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicPowerUser

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticContainerRegistryPublicReadOnly

AmazonElasticContainerRegistryPublicReadOnlyest une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule aux référentiels publics Amazon ECR.

Utilisation de cette stratégie

Vous pouvezAmazonElasticContainerRegistryPublicReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2020, 17:27 UTC
- Heure modifiée : 01 décembre 2020, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "ecr-public:GetAuthorizationToken",
    "sts:GetServiceBearerToken",
    "ecr-public:BatchCheckLayerAvailability",
    "ecr-public:GetRepositoryPolicy",
    "ecr-public:DescribeRepositories",
    "ecr-public:DescribeRegistries",
    "ecr-public:DescribeImages",
    "ecr-public:DescribeImageTags",
    "ecr-public:GetRepositoryCatalogData",
    "ecr-public:GetRegistryCatalogData"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès client root à un système de fichiers Amazon EFS

Utilisation de cette stratégie

Vous pouvez les associer AmazonElasticFileSystemClientFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 13 janvier 2020, 16:27 UTC
- Heure modifiée : 13 janvier 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemClientReadOnlyAccess

AmazonElasticFileSystemClientReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès client en lecture seule à un système de fichiers Amazon EFS

Utilisation de cette stratégie

Vous pouvez AmazonElasticFileSystemClientReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 13 janvier 2020, 16:24 UTC
- Heure modifiée : 13 janvier 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemClientReadWriteAccess

AmazonElasticFileSystemClientReadWriteAccess est une [politiqueAWS gérée](#) qui : fournit un accès client en lecture et en écriture à un système de fichiers Amazon EFS

Utilisation de cette stratégie

Vous pouvez les associer AmazonElasticFileSystemClientReadWriteAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 janvier 2020, 16:21 UTC
- Heure modifiée : 13 janvier 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemFullAccess

AmazonElasticFileSystemFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon EFS via le AWS Management Console.

Utilisation de cette politique

Vous pouvez vous associer AmazonElasticFileSystemFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2015, 16:22 UTC
- Heure modifiée : 28 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem>DeleteFileSystem",
        "elasticfilesystem>DeleteMountTarget",
        "elasticfilesystem>DeleteTags",
        "elasticfilesystem>DeleteAccessPoint",
        "elasticfilesystem>DeleteFileSystemPolicy",
        "elasticfilesystem>DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
```

```

    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups",
    "elasticfilesystem:DescribeTags",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeReplicationConfigurations",
    "elasticfilesystem:ModifyMountTargetSecurityGroups",
    "elasticfilesystem:PutAccountPreferences",
    "elasticfilesystem:PutBackupPolicy",
    "elasticfilesystem:PutLifecycleConfiguration",
    "elasticfilesystem:PutFileSystemPolicy",
    "elasticfilesystem:UpdateFileSystem",
    "elasticfilesystem:UpdateFileSystemProtection",
    "elasticfilesystem:TagResource",
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:ListTagsForResource",
    "elasticfilesystem:Backup",
    "elasticfilesystem:Restore",
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Sid" : "ElasticFileSystemFullAccess",
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Sid" : "CreateServiceLinkedRoleForEFS",
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "elasticfilesystem.amazonaws.com"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonElasticFileSystemReadOnlyAccess

AmazonElasticFileSystemReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon EFS via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonElasticFileSystemReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 mai 2015, 16:25 UTC
- Heure modifiée : 10 janvier 2022, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Action" : [
  "cloudwatch:DescribeAlarmsForMetric",
  "cloudwatch:GetMetricData",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeNetworkInterfaceAttribute",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcAttribute",
  "ec2:DescribeVpcs",
  "elasticfilesystem:DescribeAccountPreferences",
  "elasticfilesystem:DescribeBackupPolicy",
  "elasticfilesystem:DescribeFileSystems",
  "elasticfilesystem:DescribeFileSystemPolicy",
  "elasticfilesystem:DescribeLifecycleConfiguration",
  "elasticfilesystem:DescribeMountTargets",
  "elasticfilesystem:DescribeMountTargetSecurityGroups",
  "elasticfilesystem:DescribeTags",
  "elasticfilesystem:DescribeAccessPoints",
  "elasticfilesystem:DescribeReplicationConfigurations",
  "elasticfilesystem:ListTagsForResource",
  "kms:ListAliases"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemServiceRolePolicy

AmazonElasticFileSystemServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à Amazon Elastic File System de gérer les AWS ressources en votre nom

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 5 novembre 2019, 16:52 UTC
- Heure modifiée : 10 janvier 2022, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "backup:CreateBackupVault",
    "backup:PutBackupVaultAccessPolicy"
  ],
  "Resource" : [
    "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "backup:CreateBackupPlan",
    "backup:CreateBackupSelection"
  ],
  "Resource" : [
    "arn:aws:backup:*:*:backup-plan:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```

    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "backup.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateReplicationConfiguration",
    "elasticfilesystem:DescribeReplicationConfigurations",
    "elasticfilesystem>DeleteReplicationConfiguration"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticFileSystemsUtils

AmazonElasticFileSystemsUtils est une [politiqueAWS gérée](#) qui : permet aux clients d'utiliserAWS Systems Manager pour gérer automatiquement le package Amazon EFS Utilities (amazon-efs-utils) sur leurs instances EC2, et de l'utiliser CloudWatchLog pour recevoir des notifications de succès/d'échec du montage du système de fichiers EFS.

Utilisation de cette stratégie

Vous pouvezAmazonElasticFileSystemsUtils les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 septembre 2020, 15:16 UTC
- Heure modifiée : 29 septembre 2020, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2messages:AcknowledgeMessage",
      "ec2messages:DeleteMessage",
      "ec2messages:FailMessage",
      "ec2messages:GetEndpoint",
      "ec2messages:GetMessages",
      "ec2messages:SendReply"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAvailabilityZones"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups",
      "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceEditorsRole

AmazonElasticMapReduceEditorsRole est une [politique AWS gérée](#) qui : [Politique](#) par défaut pour le rôle de service Amazon Elastic MapReduce Editors.

Utilisation de cette stratégie

Vous pouvez AmazonElasticMapReduceEditorsRole les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : Politique de rôle de service
- Heure de création : 16 novembre 2018, 21:55 UTC
- Heure modifiée : 09 février 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceforAutoScalingRole

AmazonElasticMapReduceforAutoScalingRoleest une [politiqueAWS gérée](#) qui : Amazon Elastic MapReduce for Auto Scaling. Rôle permettant à Auto Scaling d'ajouter et de supprimer des instances de votre cluster EMR.

Utilisation de cette stratégie

Vous pouvez les associerAmazonElasticMapReduceforAutoScalingRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 18 novembre 2016, 01:09 UTC
- Heure modifiée : 18 novembre 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceforEC2Role

AmazonElasticMapReduceforEC2Role est une [politique AWS gérée qui : Politique](#) par défaut pour le rôle de service Amazon Elastic MapReduce pour EC2.

Utilisation de cette stratégie

Vous pouvez AmazonElasticMapReduceforEC2Role les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 11 août 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
```

```
"kinesis:PutRecord",
"kinesis:SplitShard",
"rds:Describe*",
"s3:*",
"sdb:*",
"sns:*",
"sqs:*",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue>DeleteDatabase",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:CreateTable",
"glue:UpdateTable",
"glue>DeleteTable",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersions",
"glue:CreatePartition",
"glue:BatchCreatePartition",
"glue:UpdatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:GetPartition",
"glue:GetPartitions",
"glue:BatchGetPartition",
"glue:CreateUserDefinedFunction",
"glue:UpdateUserDefinedFunction",
"glue>DeleteUserDefinedFunction",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions"
    ]
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceFullAccess

AmazonElasticMapReduceFullAccess est une [politique AWS gérée](#) qui : Cette politique est en voie d'obsolescence. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Fournit un accès complet à Amazon Elastic MapReduce et aux services sous-jacents dont il a besoin, tels que EC2 et S3

Utilisation de cette stratégie

Vous pouvez les associer AmazonElasticMapReduceFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 11 octobre 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
```

```

    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:CancelSpotInstanceRequests",
    "ec2:CreateRoute",
    "ec2:CreateSecurityGroup",
    "ec2:CreateTags",
    "ec2>DeleteRoute",
    "ec2>DeleteTags",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkAcls",
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "elasticmapreduce:*",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:List*",
    "s3:*",
    "sdb:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*"

```

```
"Condition" : {
  "StringLike" : {
    "iam:AWSServiceName" : [
      "elasticmapreduce.amazonaws.com",
      "elasticmapreduce.amazonaws.com.cn"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReducePlacementGroupPolicy

AmazonElasticMapReducePlacementGroupPolicy est une [politique AWS gérée](#) qui : Politique permettant à EMR de créer, de décrire et de supprimer des groupes de placement EC2.

Utilisation de cette stratégie

Vous pouvez les associer AmazonElasticMapReducePlacementGroupPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 septembre 2020, 00:37 UTC
- Heure modifiée : 29 septembre 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceReadOnlyAccess

AmazonElasticMapReduceReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Elastic MapReduce via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonElasticMapReduceReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 29 juillet 2020, 23h14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",

```



```
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticMapReduceRole

AmazonElasticMapReduceRole est une [politique AWS gérée](#) qui : Cette politique est en voie d'obsolescence. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Politique par défaut pour le rôle de MapReduce service Amazon Elastic.

Utilisation de cette stratégie

Vous pouvez AmazonElasticMapReduceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 24 juin 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
```

```

    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ec2:DetachNetworkInterface",
    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "ec2>DeleteVolume",
    "ec2:DescribeVolumeStatus",
    "ec2:DescribeVolumes",
    "ec2:DetachVolume",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:PassRole",
    "s3:CreateBucket",
    "s3:Get*",
    "s3:List*",
    "sdb:BatchPutAttributes",
    "sdb:Select",
    "sqs:CreateQueue",
    "sqs>Delete*",
    "sqs:GetQueue*",
    "sqs:PurgeQueue",
    "sqs:ReceiveMessage",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling>DeleteScalingPolicy",
    "application-autoscaling:Describe*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",

```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticsearchServiceRolePolicy

AmazonElasticsearchServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon Elasticsearch Service à accéder à d'autres AWS services tels que les API réseau EC2 en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 07 juillet 2017, 00:15 UTC
- Heure modifiée : 23 octobre 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    }
  ]
}
```

```
  },
  {
    "Sid" : "Stmt1480452973198",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*"
    ]
  },
  {
    "Sid" : "Stmt1480452973199",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/OpenSearchManaged" : "true"
      }
    }
  },
  {
    "Sid" : "Stmt1480452973200",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint",
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/OpenSearchManaged" : "true"
      }
    }
  },
  {
    "Sid" : "Stmt1480452973201",
    "Effect" : "Allow",
    "Action" : [
```

```
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973149",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973150",
  "Effect" : "Allow",
  "Action" : [
    "ec2:UnAssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973202",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonElasticTranscoder_FullAccess

AmazonElasticTranscoder_FullAccess est une [politique AWS gérée](#) qui : accorde aux utilisateurs un accès complet à Elastic Transcoder et l'accès aux services associés nécessaires aux fonctionnalités complètes d'Elastic Transcoder.

Utilisation de cette stratégie

Vous pouvez AmazonElasticTranscoder_FullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 avril 2018, 18:59 UTC
- Heure modifiée : 10 juin 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ]
    }
  ]
}
```



```
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "elastictranscoder.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticTranscoder_JobsSubmitter

AmazonElasticTranscoder_JobsSubmitter est une [politique AWS gérée](#) qui : autorise les utilisateurs à modifier les préférences, à soumettre des tâches et à consulter les paramètres d'Elastic Transcoder. Cette politique accorde également un accès en lecture seule à d'autres services requis pour utiliser la console Elastic Transcode, notamment S3, IAM et SNS.

Utilisation de cette stratégie

Vous pouvez AmazonElasticTranscoder_JobsSubmitter les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 juin 2018, 21:12 UTC
- Heure modifiée : 10 juin 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticTranscoder_ReadOnlyAccess

AmazonElasticTranscoder_ReadOnlyAccess est une [politique AWS gérée](#) qui : accorde aux utilisateurs un accès en lecture seule à Elastic Transcoder et un accès en liste aux services associés.

Utilisation de cette stratégie

Vous pouvez AmazonElasticTranscoder_ReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 juin 2018, 21:09 UTC
- Heure modifiée : 10 juin 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonElasticTranscoderRole

AmazonElasticTranscoderRoleest une [politiqueAWS gérée qui : Politique](#) par défaut pour le rôle de service Amazon Elastic Transcoder.

Utilisation de cette stratégie

Vous pouvez les associerAmazonElasticTranscoderRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 13 juin 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```


détails des politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 9 décembre 2020, 00:38 UTC
- Heure modifiée : 10 mars 2023, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version de stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```



```
"Action" : [
  "acm:ImportCertificate",
  "acm:AddTagsToCertificate"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "acm>DeleteCertificate"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez évoluez et évoluez de autorisations de moindre privilège et évoluez de autorisations de moindre privilège](#)

AmazonEMRFullAccessPolicy_v2

AmazonEMRFullAccessPolicy_v2 est un [AWS politique gérée](#) qui : fournit un accès complet à Amazon EMR

Utilisation de cette politique

Vous pouvez joindre AmazonEMRFullAccessPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 12 mars 2021, 01h50 UTC
- Heure modifiée :28 juillet 2023, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

Version de la politique

Version de la politique : v4(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
```

```

    "elasticmapreduce:AddTags",
    "elasticmapreduce:CancelSteps",
    "elasticmapreduce:CreateEditor",
    "elasticmapreduce:CreateSecurityConfiguration",
    "elasticmapreduce>DeleteEditor",
    "elasticmapreduce>DeleteSecurityConfiguration",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:DescribeEditor",
    "elasticmapreduce:DescribeJobFlows",
    "elasticmapreduce:DescribeSecurityConfiguration",
    "elasticmapreduce:DescribeStep",
    "elasticmapreduce:DescribeReleaseLabel",
    "elasticmapreduce:GetBlockPublicAccessConfiguration",
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:GetAutoTerminationPolicy",
    "elasticmapreduce:ListBootstrapActions",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListEditors",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "elasticmapreduce:ListSupportedInstanceTypes",
    "elasticmapreduce:ModifyCluster",
    "elasticmapreduce:ModifyInstanceFleet",
    "elasticmapreduce:ModifyInstanceGroups",
    "elasticmapreduce:OpenEditorInConsole",
    "elasticmapreduce:PutAutoScalingPolicy",
    "elasticmapreduce:PutBlockPublicAccessConfiguration",
    "elasticmapreduce:PutManagedScalingPolicy",
    "elasticmapreduce:RemoveAutoScalingPolicy",
    "elasticmapreduce:RemoveManagedScalingPolicy",
    "elasticmapreduce:RemoveTags",
    "elasticmapreduce:SetTerminationProtection",
    "elasticmapreduce:StartEditor",
    "elasticmapreduce:StopEditor",
    "elasticmapreduce:TerminateJobFlows",
    "elasticmapreduce:ViewEventsFromAllClustersInConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ViewMetricsInEMRConsole",

```

```
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PassRoleForElasticMapReduce",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
      }
    }
  },
  {
    "Sid" : "PassRoleForEC2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com*"
      }
    }
  },
  {
    "Sid" : "PassRoleForAutoScaling",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
      }
    }
  },
  {
    "Sid" : "ElasticMapReduceServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "elasticmapreduce.amazonaws.com",
          "elasticmapreduce.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleUIActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeNatGateways",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "s3:ListAllMyBuckets",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  }
]
}

```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonEMRReadOnlyAccessPolicy_v2

AmazonEMRReadOnlyAccessPolicy_v2 est un [AWS politique gérée](#) cela : fournit un accès en lecture seule à Amazon EMR et aux applications associées CloudWatch Métriques.

Utilisation de cette politique

Vous pouvez joindre AmazonEMRReadOnlyAccessPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 12 mars 2021, 01h39 UTC
- Heure modifiée : 2 août 2023, 19h15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
```

```

    "elasticmapreduce:DescribeReleaseLabel",
    "elasticmapreduce:GetBlockPublicAccessConfiguration",
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:GetAutoTerminationPolicy",
    "elasticmapreduce:ListBootstrapActions",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListEditors",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "elasticmapreduce:ListSupportedInstanceTypes",
    "elasticmapreduce:ViewEventsFromAllClustersInConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ViewMetricsInEMRConsole",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonEMRServerlessServiceRolePolicy

AmazonEMRServerlessServiceRolePolicy est une [politique AWS gérée](#) qui : autorise l'accès aux autres ressources AWS de service requises pour exécuter Amazon EMRServerless

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 20 mai 2022, 23:15 UTC
- Heure modifiée : 25 janvier 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchPolicyStatement",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/EMRServerless",
          "AWS/Usage"
        ]
      }
    }
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonEMRServicePolicy_v2

AmazonEMRServicePolicy_v2 est une [politique AWS gérée](#) qui : Cette politique est utilisée pour le rôle de service Amazon EMR et ne doit PAS être utilisée pour d'autres utilisateurs ou rôles IAM de votre compte. La politique accorde les autorisations nécessaires à la création et à la gestion des ressources associées à l'EMR et aux services connexes nécessaires au fonctionnement de votre cluster EMR.

Utilisation de cette stratégie

Vous pouvez AmazonEMRServicePolicy_v2 les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 12 mars 2021, 01:11 UTC
- Heure modifiée : 15 février 2022, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    }
  ],
}
```

```
{
  "Sid" : "CreateWithEMRTaggedLaunchTemplate",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateFleet",
    "ec2:RunInstances",
    "ec2:CreateLaunchTemplateVersion"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateEMRTaggedLaunchTemplate",
  "Effect" : "Allow",
  "Action" : "ec2:CreateLaunchTemplate",
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateEMRTaggedInstancesAndVolumes",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:CreateFleet"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
```

```

    "Sid" : "ResourcesToLaunchEC2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:CreateFleet",
      "ec2:CreateLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:image/ami-*",
      "arn:aws:ec2:*:*:key-pair/*",
      "arn:aws:ec2:*:*:capacity-reservation/*",
      "arn:aws:ec2:*:*:placement-group/EMR_*",
      "arn:aws:ec2:*:*:fleet/*",
      "arn:aws:ec2:*:*:dedicated-host/*",
      "arn:aws:resource-groups:*:*:group/*"
    ]
  },
  {
    "Sid" : "ManageEMRTaggedResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2>DeleteLaunchTemplate",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyInstanceAttribute",
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "ManageTagsOnEMRTaggedResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [

```

```

    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "TagOnCreateTaggedEMRResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateFleet",
        "CreateLaunchTemplate",

```

```
        "CreateNetworkInterface"
      ]
    }
  },
  {
    "Sid" : "TagPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:placement-group/EMR_*"
    ]
  },
  {
    "Sid" : "ListActionsForEC2Resources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribePlacementGroups",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVolumes",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
```

```
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
      "ec2:CreateAction" : "CreateSecurityGroup"
    }
  }
},
{
  "Sid" : "ManageSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateEMRPlacementGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreatePlacementGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
},
{
  "Sid" : "DeletePlacementGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeletePlacementGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScaling",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:RegisterScalableTarget"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ResourceGroupsForCapacityReservations",
  "Effect" : "Allow",

```



```

    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AutoScalingCloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
  },
  {
    "Sid" : "PassRoleForAutoScaling",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
      }
    }
  },
  {
    "Sid" : "PassRoleForEC2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonESCognitoAccess

AmazonESCognitoAccess est une [politiqueAWS gérée](#) qui : fournit un accès limité au service de configuration Amazon Cognito.

Utilisation de cette stratégie

Vous pouvez AmazonESCognitoAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 février 2018, 22:29 UTC
- Heure modifiée : 20 décembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",

```

```

    "cognito-idp:DeleteUserPoolClient",
    "cognito-idp:UpdateUserPoolClient",
    "cognito-idp:DescribeUserPoolClient",
    "cognito-idp:AdminInitiateAuth",
    "cognito-idp:AdminUserGlobalSignOut",
    "cognito-idp:ListUserPoolClients",
    "cognito-identity:DescribeIdentityPool",
    "cognito-identity:UpdateIdentityPool",
    "cognito-identity:SetIdentityPoolRoles",
    "cognito-identity:GetIdentityPoolRoles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "cognito-identity.amazonaws.com",
        "cognito-identity-us-gov.amazonaws.com"
      ]
    }
  }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonESFullAccess

AmazonESFullAccess est une [stratégie AWS gérée](#) qui : Fournit un accès complet au service de configuration Amazon ES.

Utilisation de cette stratégie

Vous pouvez associer `AmazonESFullAccess` les utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 octobre 2015, 19:14 UTC
- Heure modifiée : 01 octobre 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonESReadOnlyAccess

AmazonESReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule au service de configuration Amazon ES.

Utilisation de cette stratégie

Vous pouvez AmazonESReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 octobre 2015, 19:18 UTC
- Heure modifiée : 3 octobre 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicyest une [politiqueAWS gérée](#) qui :
Permet d'accéder EventBridge aux ressources de Secret Manager en votre nom.

Utilisation de cette politique | politique I

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom.
Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

détails détails détails détails détails

- Type : Politique de rôles liée à un service
- Heure de création : 11 février 2021, 20:52 UTC
- Heure modifiée : 11 février 2021, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec AWS politiques et évoluez vers vers vers vers vers vers vers vers vers vers vers vers vers vers vers les autorisations](#)

AmazonEventBridgeFullAccess

AmazonEventBridgeFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon EventBridge.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 juillet 2019, 14:08 UTC

- Heure modifiée : 01 décembre 2022, 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
```



```

    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "schemas.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SecretsManagerAccessForApiDestinations",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:UpdateSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:events!*"
  },
  {
    "Sid" : "IAMPassRoleAccessForEventBridge",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "events.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "IAMPassRoleAccessForScheduler",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "scheduler.amazonaws.com"
      }
    }
  },
  {

```

```
"Sid" : "IAMPassRoleAccessForPipes",
"Effect" : "Allow",
"Action" : "iam:PassRole",
"Resource" : "arn:aws:iam::*:role/*",
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : "pipes.amazonaws.com"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgePipesFullAccess

AmazonEventBridgePipesFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon EventBridge Pipes.

Utilisation de cette stratégie

Vous pouvez les associer AmazonEventBridgePipesFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2022, 17:03 UTC
- Heure modifiée : 01 décembre 2022, 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule et à un opérateur (possibilité d'arrêter et de démarrer l'exécution de Pipes) à Amazon EventBridge Pipes.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgePipesOperatorAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1er décembre 2022, 17:04 UTC
- Heure modifiée : 01 décembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgePipesReadOnlyAccess

AmazonEventBridgePipesReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon EventBridge Pipes.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgePipesReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2022, 17:04 UTC
- Heure modifiée : 01 décembre 2022, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations IAM pour l'identité](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeReadOnlyAccess

AmazonEventBridgeReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon EventBridge.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgeReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 juillet 2019, 13:59 UTC

- Heure modifiée : 01 décembre 2022, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",

```

```
    "schemas:DescribeSchema",
    "schemas:ExportSchema",
    "schemas:GetCodeBindingSource",
    "schemas:GetDiscoveredSchema",
    "schemas:GetResourcePolicy",
    "schemas:ListDiscoverers",
    "schemas:ListRegistries",
    "schemas:ListSchemas",
    "schemas:ListSchemaVersions",
    "schemas:ListTagsForResource",
    "schemas:SearchSchemas",
    "scheduler:GetSchedule",
    "scheduler:GetScheduleGroup",
    "scheduler:ListSchedules",
    "scheduler:ListScheduleGroups",
    "scheduler:ListTagsForResource",
    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeSchedulerFullAccess

AmazonEventBridgeSchedulerFullAccess est une [politiqueAWS gérée](#) qui : La politique AmazonEventBridgeSchedulerFullAccess gérée autorise l'utilisation de toutes les actions du EventBridge planificateur pour les planifications et les groupes de planification.

Utilisation de cette stratégie

Vous pouvez `AmazonEventBridgeSchedulerFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 18:37 UTC
- Heure modifiée : 10 novembre 2022, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeSchedulerReadOnlyAccess

AmazonEventBridgeSchedulerReadOnlyAccess est une [politiqueAWS gérée](#) qui : La politique AmazonEventBridgeSchedulerReadOnlyAccess gérée accorde des autorisations en lecture seule pour afficher les détails de vos calendriers et de vos groupes de planification

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgeSchedulerReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 10 novembre 2022, 18:50 UTC
- Heure modifiée : 10 novembre 2022, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeSchemasFullAccess

AmazonEventBridgeSchemasFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon EventBridge Schemas.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgeSchemasFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 28 novembre 2019, 23:12 UTC
- Heure modifiée : 28 novembre 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
```

```
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon EventBridge Schemas.

Utilisation de cette stratégie

Vous pouvez AmazonEventBridgeSchemasReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 novembre 2019, 23:05 UTC
- Heure modifiée : 01 mai 2020, 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonEventBridgeSchemasServiceRolePolicy

AmazonEventBridgeSchemasServiceRolePolicy est une [politique AWS gérée](#) qui : accorde des autorisations aux règles gérées créées par les EventBridge schémas Amazon.

En des Ides de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à un utilisateur, un groupe ou un rôle.

Obtenir les détails des détails

- Type : Politique de rôles liée à un service
- Heure de création : 27 novembre 2019, 01:10 UTC
- Heure modifiée : 27 novembre 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la version par défaut de la version qui permet à d'effectuer les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
```

```
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
    ],
    "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
    ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des AWS détails et évoluez vers les autorisations de moindre privilège](#)

AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy est une [politique AWS gérée](#) qui : Politique permettant au AWS FIS de gérer la surveillance et la sélection des ressources pour les expériences.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 décembre 2020, 21:18 UTC
- Heure modifiée : 25 octobre 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events>DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
```

```
"Effect" : "Allow",
"Action" : [
  "cloudwatch:DescribeAlarms",
  "cloudwatch:DescribeAlarmHistory"
],
"Resource" : "*"
},
{
  "Sid" : "DescribeUserResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSubnets",
    "iam:GetUser",
    "iam:GetRole",
    "iam:ListUsers",
    "iam:ListRoles",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "ecs:DescribeClusters",
    "ecs:DescribeTasks",
    "ecs:ListTasks",
    "eks:DescribeNodegroup",
    "eks:DescribeCluster"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonForecastFullAccess

AmazonForecastFullAccess est une [politiqueAWS gérée](#) qui : Donne accès à toutes les actions d'Amazon Forecast

Utilisation de cette stratégie

Vous pouvez `AmazonForecastFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 01:52 UTC
- Heure modifiée : 18 janvier 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonFraudDetectorFullAccessPolicy

AmazonFraudDetectorFullAccessPolicyest une [politiqueAWS gérée](#) qui : Donne accès à toutes les actions d'Amazon Fraud Detector

Utilisation de cette stratégie

Vous pouvez les associerAmazonFraudDetectorFullAccessPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 22:46 UTC
- Heure modifiée : 3 décembre 2019, 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "iam:PassedToService" : "frauddetector.amazonaws.com"
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonFreeRTOSFullAccess

AmazonFreeRTOSFullAccess est une [politiqueAWS gérée](#) qui : Politique d'accès complet pour Amazon FreeRTOS

Utilisation de cette stratégie

Vous pouvez AmazonFreeRTOSFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2017, 15:32 UTC
- Heure modifiée : 29 novembre 2017, 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonFreeRTOSOTAUpdate

AmazonFreeRTOSOTAUpdate est une [politique AWS gérée](#) qui : Autorise l'utilisateur à accéder à Amazon FreeRTOS OTA Update

Utilisation de cette stratégie

Vous pouvez AmazonFreeRTOSOTAUpdate les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : Politique de rôle de service
- Heure de création : 27 août 2018, 22:43 UTC
- Heure modifiée : 18 décembre 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afp-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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonFSxConsoleFullAccess

AmazonFSxConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon FSx et un accès aux AWS services associés via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonFSxConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:36 UTC
- Heure modifiée : 10 janvier 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Sid" : "FullAccessToFSx",
  "Effect" : "Allow",
  "Action" : [
    "fsx:AssociateFileGateway",
    "fsx:AssociateFileSystemAliases",
    "fsx:CancelDataRepositoryTask",
    "fsx:CopyBackup",
    "fsx:CopySnapshotAndUpdateVolume",
    "fsx>CreateBackup",
    "fsx:CreateDataRepositoryAssociation",
    "fsx:CreateDataRepositoryTask",
    "fsx:CreateFileCache",
    "fsx:CreateFileSystem",
    "fsx:CreateFileSystemFromBackup",
    "fsx:CreateSnapshot",
    "fsx:CreateStorageVirtualMachine",
    "fsx>CreateVolume",
    "fsx>CreateVolumeFromBackup",
    "fsx>DeleteBackup",
    "fsx>DeleteDataRepositoryAssociation",
    "fsx>DeleteFileCache",
    "fsx>DeleteFileSystem",
    "fsx>DeleteSnapshot",
    "fsx>DeleteStorageVirtualMachine",
    "fsx>DeleteVolume",
    "fsx:DescribeAssociatedFileGateways",
    "fsx:DescribeBackups",
    "fsx:DescribeDataRepositoryAssociations",
    "fsx:DescribeDataRepositoryTasks",
    "fsx:DescribeFileCaches",
    "fsx:DescribeFileSystemAliases",
    "fsx:DescribeFileSystems",
    "fsx:DescribeSharedVpcConfiguration",
    "fsx:DescribeSnapshots",
    "fsx:DescribeStorageVirtualMachines",
    "fsx:DescribeVolumes",
    "fsx:DisassociateFileGateway",
    "fsx:DisassociateFileSystemAliases",
    "fsx:ListTagsForResource",
    "fsx:ManageBackupPrincipalAssociations",
    "fsx:ReleaseFileSystemNfsV3Locks",
    "fsx:RestoreVolumeFromSnapshot",
    "fsx:TagResource",
```

```

    "fsx:UntagResource",
    "fsx:UpdateDataRepositoryAssociation",
    "fsx:UpdateFileCache",
    "fsx:UpdateFileSystem",
    "fsx:UpdateSharedVpcConfiguration",
    "fsx:UpdateSnapshot",
    "fsx:UpdateStorageVirtualMachine",
    "fsx:UpdateVolume"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateFSxSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CreateSLRForLustreS3Integration",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "s3.data-source.lustre.fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CreateTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [

```

```
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ManageCrossAccountDataReplication",
  "Effect" : "Allow",
  "Action" : [
    "fsx:PutResourcePolicy",
    "fsx:GetResourcePolicy",
    "fsx>DeleteResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "ram.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon FSx et un accès aux AWS services associés via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonFSxConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:35 UTC
- Heure modifiée : 10 janvier 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
```

```
    "ec2:DescribeSecurityGroups",
    "ec2:GetSecurityGroupsForVpc",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "firehose:ListDeliveryStreams",
    "fsx:Describe*",
    "fsx:ListTagsForResource",
    "kms:DescribeKey",
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonFSxFullAccess

AmazonFSxFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon FSx et un accès aux services associés AWS.

Utilisation de cette politique

Vous pouvez vous associer AmazonFSxFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:34 UTC
- Heure modifiée : 10 janvier 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx>CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx>CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx>CreateVolume",
        "fsx>CreateVolumeFromBackup",
        "fsx>DeleteBackup",
        "fsx>DeleteDataRepositoryAssociation",
        "fsx>DeleteFileCache",
```



```
    "fsx:DeleteFileSystem",
    "fsx:DeleteSnapshot",
    "fsx:DeleteStorageVirtualMachine",
    "fsx:DeleteVolume",
    "fsx:DescribeAssociatedFileGateways",
    "fsx:DescribeBackups",
    "fsx:DescribeDataRepositoryAssociations",
    "fsx:DescribeDataRepositoryTasks",
    "fsx:DescribeFileCaches",
    "fsx:DescribeFileSystemAliases",
    "fsx:DescribeFileSystems",
    "fsx:DescribeSharedVpcConfiguration",
    "fsx:DescribeSnapshots",
    "fsx:DescribeStorageVirtualMachines",
    "fsx:DescribeVolumes",
    "fsx:DisassociateFileGateway",
    "fsx:DisassociateFileSystemAliases",
    "fsx:ListTagsForResource",
    "fsx:ManageBackupPrincipalAssociations",
    "fsx:ReleaseFileSystemNfsV3Locks",
    "fsx:RestoreVolumeFromSnapshot",
    "fsx:TagResource",
    "fsx:UntagResource",
    "fsx:UpdateDataRepositoryAssociation",
    "fsx:UpdateFileCache",
    "fsx:UpdateFileSystem",
    "fsx:UpdateSharedVpcConfiguration",
    "fsx:UpdateSnapshot",
    "fsx:UpdateStorageVirtualMachine",
    "fsx:UpdateVolume"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateSLRForFSx",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fsx.amazonaws.com"
      ]
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "CreateSLRForLustreS3Integration",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "s3.data-source.lustre.fsx.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "CreateLogsForFSxWindowsAuditLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    ]
  },
  {
    "Sid" : "WriteToAmazonKinesisDataFirehose",
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    ]
  },
  {
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
```

```

    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DescribeEC2VpcResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSecurityGroups",
    "ec2:GetSecurityGroupsForVpc",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "fsx.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ManageCrossAccountDataReplication",
  "Effect" : "Allow",
  "Action" : [
    "fsx:PutResourcePolicy",
    "fsx:GetResourcePolicy",
    "fsx>DeleteResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [

```

```
        "iam.amazonaws.com"
      ]
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonFSxReadOnlyAccess

AmazonFSxReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon FSx.

Utilisation de cette stratégie

Vous pouvez AmazonFSxReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:33 UTC
- Heure modifiée : 28 novembre 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonFSxServiceRolePolicy

AmazonFSxServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon FSx à gérer les AWS ressources en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 28 novembre 2018, 10:38 UTC
- Heure modifiée : 10 janvier 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PutMetrics",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/FSx"
      }
    }
  },
  {
    "Sid" : "TagResourceNetworkInterface",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "AmazonFSx.FileSystemId"
      }
    }
  },
  {
    "Sid" : "ManageNetworkInterface",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:UnassignPrivateIpAddresses"
    ],
  },
```

```
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*"
],
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
  }
}
},
{
  "Sid" : "ManageRouteTable",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateRoute",
    "ec2:ReplaceRoute",
    "ec2>DeleteRoute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
    }
  }
},
{
  "Sid" : "PutCloudWatchLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
},
{
  "Sid" : "ManageAuditLogs",
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch"
  ]
},
```



```
    "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"  
  }  
]  
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonGlacierFullAccess

AmazonGlacierFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Glacier via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonGlacierFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGlacierReadOnlyAccess

AmazonGlacierReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Glacier via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonGlacierReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 5 mai 2016, 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGrafanaAthenaAccess

AmazonGrafanaAthenaAccess est une [politique AWS gérée](#) qui : Cette politique donne accès à Amazon Athena et aux dépendances nécessaires pour permettre d'interroger et d'écrire des résultats dans s3 à partir du plugin Amazon Athena dans Amazon Grafana.

Utilisation de cette stratégie

Vous pouvez AmazonGrafanaAthenaAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 22 novembre 2021, 17:11 UTC
- Heure modifiée : 22 novembre 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:GetWorkGroup",
      "athena:StartQueryExecution",
      "athena:StopQueryExecution"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/GrafanaDataSource" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:BatchGetPartition"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
```

```
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGrafanaCloudWatchAccess

AmazonGrafanaCloudWatchAccess est une [politique AWS gérée](#) qui : Cette politique donne accès à Amazon CloudWatch et aux dépendances nécessaires pour l'utiliser CloudWatch comme source de données dans Amazon Managed Grafana.

Utilisation de cette stratégie

Vous pouvez AmazonGrafanaCloudWatchAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 24 mars 2023, 22:41 UTC
- Heure modifiée : 24 mars 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
```

```
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "tag:GetResources",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "oam:ListSinks",
    "oam:ListAttachedLinks"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGrafanaRedshiftAccess

AmazonGrafanaRedshiftAccess est une [politique AWS gérée](#) qui : Cette politique accorde un accès limité à Amazon Redshift et aux dépendances nécessaires à l'utilisation du plugin Amazon Redshift dans Amazon Grafana.

Utilisation de cette stratégie

Vous pouvez AmazonGrafanaRedshiftAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 26 novembre 2021, 23h15 UTC
- Heure modifiée : 26 novembre 2021, 23h15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/**",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : fournit un accès aux AWS ressources gérées ou utilisées par Amazon Grafana.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 8 novembre 2022, 23:10 UTC
- Heure modifiée : 8 novembre 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "Null" : {
      "aws:RequestTag/AmazonGrafanaManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:DeleteNetworkInterface",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet pour utiliser Amazon GuardDuty.

Utilisation de cette politique

Vous pouvez vous associer `AmazonGuardDutyFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 22:31 UTC
- Heure modifiée : 16 novembre 2023, 23h04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
},
{
  "Sid" : "ActionsForOrganizationsSid1",
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IamGetRoleSid1",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

AmazonGuardDutyMalwareProtectionServiceRolePolicy est une [politique AWS gérée](#) selon laquelle : la protection contre les GuardDuty programmes malveillants utilise le rôle lié au service

(SLR) nommé. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ce rôle lié au service permet à la protection contre les GuardDuty programmes malveillants d'effectuer des analyses sans agent pour détecter les logiciels malveillants. Il permet GuardDuty de créer des instantanés dans votre compte et de partager les instantanés avec le compte de GuardDuty service pour détecter les logiciels malveillants. Il évalue ces instantanés partagés et inclut les métadonnées de l'instance EC2 récupérées dans les résultats de la protection GuardDuty contre les logiciels malveillants. Le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service fait confiance au service `malware-protection.guardduty.amazonaws.com` pour assumer le rôle.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 19 juillet 2022, 19:06 UTC
- Heure modifiée : 25 janvier 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTasks",
    "ecs:DescribeTasks",
    "eks:DescribeCluster"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateSnapshotVolumeConditionalStatement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshot",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
},
{
  "Sid" : "CreateSnapshotConditionalStatement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshot",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyScanId"
    }
  }
},
{
  "Sid" : "CreateTagsPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:*/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateSnapshot"
    }
  }
},

```



```
{
  "Sid" : "AddTagsToSnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/GuardDutyScanId" : "*"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "GuardDutyExcluded",
        "GuardDutyFindingDetected"
      ]
    }
  }
},
{
  "Sid" : "DeleteAndShareSnapshotPermission",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot",
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/GuardDutyScanId" : "*"
    },
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
},
{
  "Sid" : "PreventPublicAccessToSnapshotPermission",
  "Effect" : "Deny",
  "Action" : [
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:Add/group" : "all"
    }
  }
}
```

```

    }
  }
},
{
  "Sid" : "CreateGrantPermission",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
},
{
  "Sid" : "ShareSnapshotKMSPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    },
    "Null" : {

```

```

        "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
}
},
{
    "Sid" : "DescribeKeyPermission",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "arn:aws:kms:*:*:key/*"
},
{
    "Sid" : "GuardDutyLogGroupPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/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"
        }
    }
}

```

```
    }  
  }  
} ]  
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux GuardDuty ressources Amazon

Utilisation de cette politique

Vous pouvez vous associer AmazonGuardDutyReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 22:29 UTC
- Heure modifiée : 16 novembre 2023, 23h07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonGuardDutyServiceRolePolicy

AmazonGuardDutyServiceRolePolicy est une [politique AWS gérée](#) qui : autorise l'accès aux AWS ressources utilisées ou gérées par Amazon Guard Duty

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 28 novembre 2017, 20:12 UTC
- Heure modifiée : 9 février 2024, 18h30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",

```

```

    "s3:GetEncryptionConfiguration",
    "s3:GetBucketTagging",
    "s3:GetAccountPublicAccessBlock",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "lambda:GetFunctionConfiguration",
    "lambda:ListTags",
    "eks:ListClusters",
    "eks:DescribeCluster",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeSecurityGroups",
    "ecs:ListClusters",
    "ecs:DescribeClusters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GuardDutyCreateSLRPolicy",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
    }
  }
},
{
  "Sid" : "GuardDutyCreateVpcEndpointPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    },
    "StringLike" : {
      "ec2:VpceServiceName" : [
        "com.amazonaws.*.guardduty-data",
        "com.amazonaws.*.guardduty-data-fips"
      ]
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint",
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/GuardDutyManaged" : false
      }
    }
  }
},
{
  "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
}
},
{
```



```

    "Sid" : "GuardDutySecurityGroupManagementPolicy",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/GuardDutyManaged" : false
      }
    }
  },
  {
    "Sid" : "GuardDutyCreateSecurityGroupPolicy",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSecurityGroup",
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/GuardDutyManaged" : "*"
      }
    }
  },
  {
    "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSecurityGroup",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "GuardDutyManaged"
      }
    }
  }
}

```

```

    }
  }
},
{
  "Sid" : "GuardDutyCreateEksAddonPolicy",
  "Effect" : "Allow",
  "Action" : "eks:CreateAddon",
  "Resource" : "arn:aws:eks:*:*:cluster/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutyEksAddonManagementPolicy",
  "Effect" : "Allow",
  "Action" : [
    "eks>DeleteAddon",
    "eks:UpdateAddon",
    "eks:DescribeAddon"
  ],
  "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
},
{
  "Sid" : "GuardDutyEksClusterTagResourcePolicy",
  "Effect" : "Allow",
  "Action" : "eks:TagResource",
  "Resource" : "arn:aws:eks:*:*:cluster/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
  "Effect" : "Allow",
  "Action" : "ecs:PutAccountSettingDefault",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:account-setting" : [
        "guardDutyActivate"
      ]
    }
  }
}

```

```
    ]
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonHealthLakeFullAccess

AmazonHealthLakeFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet au HealthLake service Amazon.

Utilisation de cette stratégie

Vous pouvez AmazonHealthLakeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 01:07 UTC
- Heure modifiée : 17 février 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule au HealthLake service Amazon.

Utilisation de cette stratégie

Vous pouvez `AmazonHealthLakeReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 02:43 UTC
- Heure modifiée : 17 février 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeFullAccess

AmazonHoneycodeFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Honeycode via leAWS Management Console et le SDK.

Utilisation de cette stratégie

Vous pouvezAmazonHoneycodeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 24 juin 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Action" : [
      "honeycode:*"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Honeycode via leAWS Management Console et le SDK.

Utilisation de cette stratégie

Vous pouvezAmazonHoneycodeReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy est une [politique AWS gérée](#) qui : Un rôle lié à un service est requis pour qu'Amazon Honeycode puisse accéder à vos ressources.

Utilisation de cette politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 18 novembre 2020, 18:03 UTC
- Heure modifiée : 18 novembre 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations de politique est la version qui définit les autorisations pour la politique est la version qui définit les autorisations pour Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez les autorisations de moindre privilège des autorisations de moindre privilège des autorisations de moindre privilège des autorisations de](#)

AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Honeycode Team Association via le SDK AWS Management Console et.

Utilisation de cette stratégie

Vous pouvez AmazonHoneycodeTeamAssociationFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 24 juin 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
 ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

AmazonHoneycodeTeamAssociationReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Honeycode Team Association via le SDKAWS Management Console et.

Utilisation de cette stratégie

Vous pouvezAmazonHoneycodeTeamAssociationReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2020, 20:27 UTC
- Heure modifiée : 24 juin 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeWorkbookFullAccess

AmazonHoneycodeWorkbookFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet au manuel Honeycode via le SDKAWS Management Console et.

Utilisation de cette stratégie

Vous pouvez les associer AmazonHoneycodeWorkbookFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17h30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonHoneycodeWorkbookReadOnlyAccess

AmazonHoneycodeWorkbookReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule au manuel Honeycode via le SDKAWS Management Console et.

Utilisation de cette stratégie

Vous pouvez AmazonHoneycodeWorkbookReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonInspector2AgentlessServiceRolePolicy

AmazonInspector2AgentlessServiceRolePolicy est une [politique AWS gérée](#) qui : accorde à Amazon Inspector l'accès Services AWS nécessaire pour effectuer des évaluations de sécurité sans agent

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 20 novembre 2023, 15:18 UTC
- Heure modifiée : 20 novembre 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume*"
      ]
    }
  ],
  {
```



```
"Sid" : "DenyCreateSnapshotsOnExcludedInstances",
"Effect" : "Deny",
"Action" : "ec2:CreateSnapshots",
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "StringEquals" : {
    "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
  }
},
{
  "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:TagKeys" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "InspectorScan"
    }
  }
},
{
  "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:CreateAction" : "CreateSnapshots"
    },
    "Null" : {
      "aws:TagKeys" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "InspectorScan"
    }
  }
},
{
  "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
  "Effect" : "Allow",
```

```

    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/InspectorScan" : "*"
      }
    }
  },
  {
    "Sid" : "DenyKmsDecryptForExcludedKeys",
    "Effect" : "Deny",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/InspectorEc2Exclusion" : "true"
      }
    }
  },
  {
    "Sid" : "DecryptSnapshotBlocksVolContext",
    "Effect" : "Allow",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "StringLike" : {
        "kms:ViaService" : "ec2.*.amazonaws.com",
        "kms:EncryptionContext:aws:ebs:id" : "vol-*"
      }
    }
  },
  {
    "Sid" : "DecryptSnapshotBlocksSnapContext",
    "Effect" : "Allow",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "StringLike" : {

```

```
        "kms:ViaService" : "ec2.*.amazonaws.com",
        "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    }
}
},
{
    "Sid" : "DescribeKeysForEbsOperations",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
            "kms:ViaService" : "ec2.*.amazonaws.com"
        }
    }
},
{
    "Sid" : "ListKeyResourceTags",
    "Effect" : "Allow",
    "Action" : "kms:ListResourceTags",
    "Resource" : "arn:aws:kms:*:*:key/*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonInspector2FullAccess

AmazonInspector2FullAccess est un [AWS politique gérée](#) cela : fournit un accès complet à Amazon Inspector et à d'autres services connexes tels que les organisations.

Utilisation de cette politique

Vous pouvez joindre AmazonInspector2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 29 novembre 2021, 19h10 UTC
- Heure modifiée :3 août 2023, 19h28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

Version de la politique

Version de la politique : v3(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "inspector2.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonInspector2ManagedCisPolicy

AmazonInspector2ManagedCisPolicy est une [politique AWS gérée](#) qui : Il s'agit d'une politique gérée que le client doit associer à ses rôles pour communiquer avec le service d'inspection pour les scans CIS

Utilisation de cette politique

Vous pouvez vous associer AmazonInspector2ManagedCisPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 24 janvier 2024, 16:31 UTC
- Heure modifiée : 24 janvier 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonInspector2ReadOnlyAccess

AmazonInspector2ReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule au service Amazon Inspector2 et aux services de support pertinents

Utilisation de cette politique

Vous pouvez vous associer AmazonInspector2ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 janvier 2022, 14:45 UTC
- Heure modifiée : 22 septembre 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",

```

```
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonInspector2ServiceRolePolicy

AmazonInspector2ServiceRolePolicy est une [politique AWS gérée](#) qui : accorde à Amazon Inspector l'accès aux éléments Services AWS nécessaires pour effectuer des évaluations de sécurité

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 16 novembre 2021, 20:27 UTC
- Heure modifiée : 22 janvier 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",

```

```

    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PackageVulnerabilityScanning",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
    "ecr:DescribeRegistry",
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",

```

```

    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaPackageVulnerabilityScanning",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions",
    "lambda:GetFunction",
    "lambda:GetLayerVersion",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GatherInventory",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "ssm>DeleteAssociation",
    "ssm:UpdateAssociation"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonInspector2-*",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:association/*"
  ]
},
{
  "Sid" : "DataSyncCleanup",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateResourceDataSync",

```

```
    "ssm:DeleteResourceDataSync"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
  ]
},
{
  "Sid" : "ManagedRules",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events>DeleteRule",
    "events:DescribeRule",
    "events>ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
  ]
},
{
  "Sid" : "LambdaCodeVulnerabilityScanning",
  "Effect" : "Allow",
  "Action" : [
    "codeguru-security:CreateScan",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:GetFindings",
    "codeguru-security:GetScan",
    "codeguru-security>ListFindings",
    "codeguru-security:BatchGetFindings",
    "codeguru-security>DeleteScansByCategory"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "CodeGuruCodeVulnerabilityScanning",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetPolicy",
```

```

    "iam:GetPolicyVersion",
    "iam:ListAttachedRolePolicies",
    "iam:ListPolicies",
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "codeguru-security.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "Ec2DeepInspection",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm:GetParameters",
    "ssm>DeleteParameter"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowManagementOfServiceLinkedChannel",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateServiceLinkedChannel",
    "cloudtrail>DeleteServiceLinkedChannel"
  ],
  "Resource" : [

```

```
    "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowListServiceLinkedChannels",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:ListServiceLinkedChannels"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowToRunInvokeCisSpecificDocuments",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
  ]
},
{
  "Sid" : "AllowToRunCisCommandsToSpecificResources",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  },
  {
    "Sid" : "AllowToPutCloudwatchMetricData",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/Inspector2"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonInspectorFullAccess

AmazonInspectorFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon Inspector.

Utilisation de cette stratégie

Vous pouvez AmazonInspectorFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 7 octobre 2015, 17:08 UTC
- Heure modifiée : 21 décembre 2017, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```



```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "inspector.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonInspectorReadOnlyAccess

AmazonInspectorReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Inspector.

Utilisation de cette stratégie

Vous pouvez AmazonInspectorReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 octobre 2015, 17:08 UTC
- Heure modifiée : 01 octobre 2019, 15:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonInspectorServiceRolePolicy

AmazonInspectorServiceRolePolicy est une [politique AWS gérée](#) qui : accorde à Amazon Inspector l'accès aux informations Services AWS nécessaires pour effectuer des évaluations de sécurité

Using this policy

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les stratégies à vos utilisateurs,

les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 novembre 2017, 15:48 UTC
- Heure modifiée : 11 septembre 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La politique est la politique qui définit les stratégies Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

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" : "*"
}
]

```

```
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS](#)

AmazonKendraFullAccess

AmazonKendraFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Kendra via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonKendraFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 16:15 UTC
- Heure modifiée : 3 décembre 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Action" : "iam:PassRole",
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "kendra.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:DescribeSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
},
{
  "Effect" : "Allow",
  "Action" : "kendra:*",
  "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKendraReadOnlyAccess

AmazonKendraReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Kendra via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez `AmazonKendraReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 16:13 UTC
- Heure modifiée : 27 mai 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKeyspacesFullAccess

AmazonKeyspacesFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Keyspaces

Utilisation de cette politique

Vous pouvez vous associer AmazonKeyspacesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 avril 2020, 17:06 UTC
- Heure modifiée : 3 octobre 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Sid" : "CassandraFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "cassandra:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ApplicationAutoscalingFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DeleteScheduledAction",
      "application-autoscaling:DeregisterScalableTarget",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingActivities",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:DescribeScheduledActions",
      "application-autoscaling:PutScheduledAction",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:RegisterScalableTarget",
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudwatchAlarmsFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ApplicationAutoscalingServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
    "Condition" : {

```

```

    "StringLike" : {
      "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
    }
  },
  {
    "Sid" : "KeyspacesReplicationServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "Ec2VpcReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonKeyspacesReadOnlyAccess

AmazonKeyspacesReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Keyspaces

Utilisation de cette stratégie

Vous pouvez `AmazonKeyspacesReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 avril 2020, 17:07 UTC
- Heure modifiée : 07 juillet 2022, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKeyspacesReadOnlyAccess_v2

AmazonKeyspacesReadOnlyAccess_v2 est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Keyspaces et aux services associés AWS.

Utilisation de cette politique

Vous pouvez vous associer AmazonKeyspacesReadOnlyAccess_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 septembre 2023, 17:01 UTC
- Heure modifiée : 12 septembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonKinesisAnalyticsFullAccess

AmazonKinesisAnalyticsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Kinesis Analytics via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer AmazonKinesisAnalyticsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 septembre 2016, 19:01 UTC
- Heure modifiée : 21 septembre 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisAnalyticsReadOnly

AmazonKinesisAnalyticsReadOnlyest une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Kinesis Analytics via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonKinesisAnalyticsReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 septembre 2016, 18:16 UTC
- Heure modifiée : 21 septembre 2016, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
    "Effect" : "Allow",
    "Action" : "logs:GetLogEvents",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicyVersions",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisFirehoseFullAccess

AmazonKinesisFirehoseFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à tous les flux de diffusion Amazon Kinesis Firehose.

Utilisation de cette stratégie

Vous pouvez les associer AmazonKinesisFirehoseFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 octobre 2015, 18:45 UTC
- Heure modifiée : 7 octobre 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisFirehoseReadOnlyAccess

AmazonKinesisFirehoseReadOnlyAccessest une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à tous les flux de diffusion Amazon Kinesis Firehose.

Utilisation de cette stratégie

Vous pouvezAmazonKinesisFirehoseReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 octobre 2015, 18:43 UTC
- Heure modifiée : 7 octobre 2015, 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisFullAccess

AmazonKinesisFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à tous les flux via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonKinesisFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisReadOnlyAccess

AmazonKinesisReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à tous les flux via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonKinesisReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisVideoStreamsFullAccess

AmazonKinesisVideoStreamsFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon Kinesis Video Streams via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonKinesisVideoStreamsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2017, 23:27 UTC
- Heure modifiée : 01 décembre 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonKinesisVideoStreamsReadOnlyAccess

AmazonKinesisVideoStreamsReadOnlyAccessest une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule àAWS Kinesis Video Streams via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonKinesisVideoStreamsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2017, 23:14 UTC
- Heure modifiée : 01 décembre 2017, 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLaunchWizard_Fullaccess

AmazonLaunchWizard_Fullaccess est une [politique AWS gérée](#) qui : Accès complet à l'assistant deAWS lancement et aux autres services requis.

Utilisation de cette stratégie

Vous pouvez AmazonLaunchWizard_Fullaccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 août 2020, 17:47 UTC
- Heure modifiée : 22 février 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
```

```
"Effect" : "Allow",
"Action" : [
  "route53:ChangeResourceRecordSets",
  "route53:GetChange",
  "route53:ListResourceRecordSets",
  "route53:ListHostedZones",
  "route53:ListHostedZonesByName"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
```

```
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AllocateHosts",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:CreateDhcpOptions",
    "ec2:CreateEgressOnlyInternetGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateVolume",
    "ec2:CreateVpcEndpoint",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVolumeAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:AssociateDhcpOptions",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:AttachVolume",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteKeyPair",
    "ec2>DeleteNatGateway",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteVolume",
    "ec2>DeleteVpc",
    "ec2:DetachInternetGateway",
    "ec2:DetachVolume",
    "ec2>DeleteSnapshot",
    "ec2:AssociateRouteTable",
    "ec2:AssociateVpcCidrBlock",
    "ec2>DeleteNetworkAcl",
    "ec2>DeleteNetworkInterface",
```

```

    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DeleteRoute",
    "ec2:DeleteRouteTable",
    "ec2:DeleteSubnet",
    "ec2:DetachNetworkInterface",
    "ec2:DisassociateAddress",
    "ec2:DisassociateVpcCidrBlock",
    "ec2:GetLaunchTemplateData",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:GetConsoleOutput",
    "ec2:GetPasswordData",
    "ec2:ReleaseAddress",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem:DeleteFileSystem",
    "elasticfilesystem:DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [

```

```

    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",
    "cloudformation>DeleteStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
    "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/**"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:AddRoleToInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
    "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [

```

```

    "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
    "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
    "arn:aws:iam::*:instance-profile/LaunchWizard*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:CreateOrUpdateTags",
    "logs:CreateLogStream",
    "logs>DeleteLogGroup",
    "logs>DeleteLogStream",
    "logs:DescribeLog*",
    "logs:PutLogEvents",
    "resource-groups:CreateGroup",
    "resource-groups>DeleteGroup",
    "sns:ListSubscriptionsByTopic",
    "sns:Publish",
    "ssm>DeleteDocument",
    "ssm>DeleteParameter*",
    "ssm:DescribeDocument*",
    "ssm:GetDocument",
    "ssm:PutParameter"
  ],
  "Resource" : [
    "arn:aws:resource-groups::*:group/LaunchWizard*",
    "arn:aws:sns::*:*",
    "arn:aws:autoscaling::*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*"
  ]
}

```



```

    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
    "arn:aws:ssm:*:*:parameter/LaunchWizard*",
    "arn:aws:ssm:*:*:document/LaunchWizard*",
    "arn:aws:logs:*:*:log-group:*:*:*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-RunShellScript"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DeleteLogStream",
    "logs:GetLogEvents",
    "logs:PutLogEvents",
    "ssm:AddTagsToResource",
    "ssm:DescribeDocument",
    "ssm:GetDocument",
    "ssm:ListTagsForResource",
    "ssm:RemoveTagsFromResource"
  ]
}

```

```
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
```

```

    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "logs:GetLog*",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*:*:*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:List*",
    "cloudformation:Describe*"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {

```

```
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "autoscaling.amazonaws.com",
        "application-insights.amazonaws.com",
        "events.amazonaws.com",
        "autoscaling.amazonaws.com.cn",
        "events.amazonaws.com.cn"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "launchwizard:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:TagQueue",
      "sqs:GetQueueUrl",
      "sqs:AddPermission",
      "sqs:ListQueues",
      "sqs>DeleteQueue",
      "sqs:GetQueueAttributes",
      "sqs:ListQueueTags",
      "sqs>CreateQueue",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "iam:GetInstanceProfile",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "route53:ListHostedZones",
    "ec2:CreateSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateFileSystem",
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:s3:::launchwizard*/**",
    "arn:aws:s3:::aws-sap-data-provider/config.properties"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "cloudformation:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3>DeleteBucket",
    "lambda:CreateFunction",
```

```

    "lambda:DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:LaunchWizard*",
    "arn:aws:s3:::launchwizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager>ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager>ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [

```

```

    "ssm:CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:DeleteOpsMetadata",
  "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:UntagResource",
    "fsx:TagResource",
    "fsx>DeleteFileSystem",
    "fsx:ListTagsForResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/Name" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:CreateFileSystem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/Name" : [
        "LaunchWizard*"
      ]
    }
  }
}

```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:CreatePortfolio",
    "servicecatalog:DescribePortfolio",
    "servicecatalog:CreateConstraint",
    "servicecatalog:CreateProduct",
    "servicecatalog:AssociatePrincipalWithPortfolio",
    "servicecatalog:CreateProvisioningArtifact",
    "servicecatalog:TagResource",
    "servicecatalog:UntagResource"
  ],
  "Resource" : [
    "arn:aws:servicecatalog:*:*:*/*",
    "arn:aws:catalog:*:*:*/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor0",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm>DeleteAssociation"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}
```



```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:TagResource"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:TagResource",
    "logs:UntagResource"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLaunchWizardFullAccessV2

AmazonLaunchWizardFullAccessV2 est un [AWS politique gérée](#) qui : Accès complet à AWS Assistant de lancement et autres services requis.

Utilisation de cette politique

Vous pouvez joindre AmazonLaunchWizardFullAccessV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 01 septembre 2023, 17h14 UTC
- Heure modifiée : 01 septembre 2023, 17h14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "Route53Actions0",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeResourceRecordSets",
      "route53:GetChange",
      "route53:ListResourceRecordSets",
      "route53:ListHostedZones",
      "route53:ListHostedZonesByName"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3Actions0",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsActions0",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchActions0",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:List*",
      "cloudwatch:Get*",
      "cloudwatch:Describe*"
    ],
    "Resource" : "*"
  },
  {
```

```
"Sid" : "Ec2Actions0",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateInternetGateway",
  "ec2:CreateNatGateway",
  "ec2:CreateVpc",
  "ec2:CreateKeyPair",
  "ec2:CreateRoute",
  "ec2:CreateRouteTable",
  "ec2:CreateSubnet"
],
"Resource" : "*"
},
{
  "Sid" : "Ec2Actions1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AllocateHosts",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:CreateDhcpOptions",
    "ec2:CreateEgressOnlyInternetGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateVolume",
    "ec2:CreateVpcEndpoint",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVolumeAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:AssociateDhcpOptions",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:AttachVolume",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteKeyPair",
    "ec2>DeleteNatGateway",
    "ec2>DeleteSecurityGroup",
```

```
"ec2:DeleteVolume",
"ec2:DeleteVpc",
"ec2:DetachInternetGateway",
"ec2:DetachVolume",
"ec2:DeleteSnapshot",
"ec2:AssociateRouteTable",
"ec2:AssociateVpcCidrBlock",
"ec2:DeleteNetworkAcl",
"ec2:DeleteNetworkInterface",
"ec2:DeleteNetworkInterfacePermission",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DeleteSubnet",
"ec2:DetachNetworkInterface",
"ec2:DisassociateAddress",
"ec2:DisassociateVpcCidrBlock",
"ec2:GetLaunchTemplateData",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolume",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:GetConsoleOutput",
"ec2:GetPasswordData",
"ec2:ReleaseAddress",
"ec2:ReplaceRoute",
"ec2:ReplaceRouteTableAssociation",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:DisassociateIamInstanceProfile",
"ec2:DisassociateRouteTable",
"ec2:DisassociateSubnetCidrBlock",
"ec2:ModifyInstancePlacement",
"ec2:DeletePlacementGroup",
"ec2:CreatePlacementGroup",
"elasticfilesystem:DeleteFileSystem",
"elasticfilesystem:DeleteMountTarget",
"ds:AddIpRoutes",
"ds:CreateComputer",
"ds:CreateMicrosoftAD",
"ds:DeleteDirectory",
"servicecatalog:AssociateProductWithPortfolio",
"cloudformation:GetTemplateSummary",
"sts:GetCallerIdentity"
],
"Resource" : "*",
```

```
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudFormationActions0",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStack*",
      "cloudformation:Get*",
      "cloudformation:ListStacks",
      "cloudformation:SignalResource",
      "cloudformation>DeleteStack"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
      "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
    ]
  },
  {
    "Sid" : "Ec2Actions2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/**"
      }
    }
  },
  {
    "Sid" : "IamActions0",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:AddRoleToInstanceProfile"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
      "arn:aws:iam::*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Sid" : "IamActions1",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
      "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
      "arn:aws:iam::*:instance-profile/LaunchWizard*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com",
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Sid" : "AutoScalingActions0",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:CreateOrUpdateTags",
      "resource-groups:CreateGroup",
      "resource-groups>DeleteGroup",
      "sns:ListSubscriptionsByTopic",
      "sns:Publish",
      "ssm>DeleteDocument",
      "ssm>DeleteParameter*"
    ]
  }
}
```

```

    "ssm:DescribeDocument*",
    "ssm:GetDocument",
    "ssm:PutParameter"
  ],
  "Resource" : [
    "arn:aws:resource-groups:*:*:group/LaunchWizard*",
    "arn:aws:sns:*:*:*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
    "arn:aws:ssm:*:*:parameter/LaunchWizard*",
    "arn:aws:ssm:*:*:document/LaunchWizard*"
  ]
},
{
  "Sid" : "SsmActions0",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-RunShellScript"
  ]
},
{
  "Sid" : "SsmActions1",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    }
  }
},
{
  "Sid" : "SsmActions2",

```



```
"Effect" : "Allow",
"Action" : [
  "ssm:AddTagsToResource",
  "ssm:DescribeDocument",
  "ssm:GetDocument",
  "ssm:ListTagsForResource",
  "ssm:RemoveTagsFromResource"
],
"Resource" : [
  "arn:aws:ssm:*:*:parameter/LaunchWizard*",
  "arn:aws:ssm:*:*:document/LaunchWizard*"
]
},
{
  "Sid" : "SsmActions3",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*",
    "cloudformation:DescribeAccountLimits",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:List*",
    "cloudformation:ValidateTemplate",
    "ds:Describe*",
    "ds:ListAuthorizedApplications",
    "ec2:Describe*",
    "ec2:Get*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:List*",
    "resource-groups:Get*",
    "resource-groups:List*",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListServiceQuotas",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "ssm:CreateDocument",
    "ssm:DescribeAutomation*",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeParameters",
    "ssm:GetAutomationExecution",
    "ssm:GetCommandInvocation",
```

```

    "ssm:GetParameter*",
    "ssm:GetConnectionStatus",
    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudFormationActions1",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:List*",
    "cloudformation:Describe*"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
},
{
  "Sid" : "IamActions2",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "autoscaling.amazonaws.com",

```

```

        "application-insights.amazonaws.com",
        "events.amazonaws.com",
        "autoscaling.amazonaws.com.cn",
        "events.amazonaws.com.cn"
    ]
}
},
{
    "Sid" : "LaunchWizardActions0",
    "Effect" : "Allow",
    "Action" : "launchwizard:*",
    "Resource" : "*"
},
{
    "Sid" : "SqsActions0",
    "Effect" : "Allow",
    "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs>DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs>CreateQueue",
        "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
},
{
    "Sid" : "CloudWatchActions1",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
},

```

```
{
  "Sid" : "EfsActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "route53:ListHostedZones",
    "ec2:CreateSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateFileSystem",
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3Actions1",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:s3:::launchwizard*/**",
    "arn:aws:s3:::aws-sap-data-provider/config.properties"
  ]
},
{
  "Sid" : "CloudFormationActions2",
  "Effect" : "Allow",
  "Action" : "cloudformation:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
},
{
  "Sid" : "LambdaActions0",
  "Effect" : "Allow",
  "Action" : [
```

```

    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3>DeleteBucket",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:LaunchWizard*",
    "arn:aws:s3:::launchwizard*"
  ]
},
{
  "Sid" : "DynamodbActions0",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Sid" : "SecretsManagerActions0",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Sid" : "SecretsManagerActions1",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",

```

```
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions5",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions6",
  "Effect" : "Allow",
  "Action" : "ssm:DeleteOpsMetadata",
  "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
},
{
  "Sid" : "SnsActions0",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
},
{
  "Sid" : "FsxActions0",
  "Effect" : "Allow",
  "Action" : [
    "fsx:UntagResource",
    "fsx:TagResource",
    "fsx>DeleteFileSystem",
    "fsx:ListTagsForResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/Name" : "LaunchWizard*"
    }
  }
}
```

```

},
{
  "Sid" : "FsxActions1",
  "Effect" : "Allow",
  "Action" : [
    "fsx:CreateFileSystem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/Name" : [
        "LaunchWizard*"
      ]
    }
  }
},
{
  "Sid" : "FsxActions2",
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ServiceCatalogActions0",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:CreatePortfolio",
    "servicecatalog:DescribePortfolio",
    "servicecatalog:CreateConstraint",
    "servicecatalog:CreateProduct",
    "servicecatalog:AssociatePrincipalWithPortfolio",
    "servicecatalog:CreateProvisioningArtifact",
    "servicecatalog:TagResource",
    "servicecatalog:UntagResource"
  ],
  "Resource" : [
    "arn:aws:servicecatalog:*:*:*/*",
    "arn:aws:catalog:*:*:*/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "SsmActions7",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm>DeleteAssociation"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "arn:aws:ssm:*:*:association/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "EfsActions1",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:TagResource"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "LogsActions0",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs>DeleteLogGroup",
    "logs:DescribeLogStreams",
    "logs:UntagResource",
    "logs:TagResource",
    "logs>CreateLogGroup",
```



```

    "logs:DeleteLogStream",
    "logs:PutLogEvents",
    "logs:GetLogEvents",
    "logs:GetLogDelivery",
    "logs:GetLogGroupFields",
    "logs:GetLogRecord",
    "logs:ListLogDeliveries"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:LaunchWizard*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "LogsActions1",
  "Effect" : "Allow",
  "Action" : "logs:DescribeLogGroups",
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "FsxActions3",
  "Effect" : "Allow",
  "Action" : [
    "fsx:CreateStorageVirtualMachine",
    "fsx:CreateVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [

```

```

        "launchwizard.amazonaws.com"
    ]
  }
},
{
  "Sid" : "FsxActions4",
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeStorageVirtualMachines",
    "fsx:DescribeVolumes"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "launchwizard.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "FsxActions5",
  "Effect" : "Allow",
  "Action" : [
    "fsx>DeleteStorageVirtualMachine",
    "fsx>DeleteVolume"
  ],
  "Resource" : [
    "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
    "arn:aws:fsx:*:*:backup/*",
    "arn:aws:fsx:*:*:volume/*/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "launchwizard.amazonaws.com"
      ]
    }
  }
}
}

```

```

    }
  ]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations du moindre privilège](#)

AmazonLexChannelsAccess

AmazonLexChannelsAccess est une [politiqueAWS gérée](#) qui : Cette politique permet aux clients d'appeler Lex Runtime à partir de canaux

Utilisation des des des des des des

Cette stratégie est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, les les les les les les les les les les les les les les les les les

les des des des des

- Type : Politique de rôles liée à un service
- Heure de création : 13 janvier 2021, 20:12 UTC
- Heure modifiée : 13 janvier 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui permet à les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

d'un document de politique JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des des des des des des des actions AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLexFullAccess

AmazonLexFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Lex via le AWS Management Console. Permet également de créer des rôles liés au service Lex et d'accorder à Lex les autorisations nécessaires pour invoquer un ensemble limité de fonctions Lambda.

Utilisation de cette politique

Vous pouvez vous associer AmazonLexFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:20 UTC
- Heure modifiée : 7 février 2024, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
    "Condition" : {
        "StringEquals" : {
            "lambda:Principal" : "lex.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement3",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam:*:*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam:*:*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam:*:*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam:*:*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
},
{
    "Sid" : "AmazonLexFullAccessStatement4",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "lex.amazonaws.com"
        }
    }
},
{

```

```
    "Sid" : "AmazonLexFullAccessStatement5",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "channels.lex.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement6",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement7",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
      }
    }
  }
}
```

```

    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement8",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement9",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
      "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
  },
  {
    "Sid" : "AmazonLexFullAccessStatement10",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ]
  }
}

```



```

    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lex.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement11",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lexv2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement12",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [

```

```
        "channels.lexv2.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement13",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lexv2.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonLexReadOnly

AmazonLexReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Lex.

Utilisation de cette stratégie

Vous pouvez AmazonLexReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:13 UTC
- Heure modifiée : 31 janvier 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
```

```

    "lex:GetSlotType",
    "lex:GetSlotTypes",
    "lex:GetSlotTypeVersions",
    "lex:GetUtterancesView",
    "lex:DescribeBot",
    "lex:DescribeBotAlias",
    "lex:DescribeBotChannel",
    "lex:DescribeBotLocale",
    "lex:DescribeBotRecommendation",
    "lex:DescribeBotVersion",
    "lex:DescribeExport",
    "lex:DescribeImport",
    "lex:DescribeIntent",
    "lex:DescribeResourcePolicy",
    "lex:DescribeSlot",
    "lex:DescribeSlotType",
    "lex:ListBots",
    "lex:ListBotLocales",
    "lex:ListBotAliases",
    "lex:ListBotChannels",
    "lex:ListBotRecommendations",
    "lex:ListBotVersions",
    "lex:ListBuiltInIntents",
    "lex:ListBuiltInSlotTypes",
    "lex:ListExports",
    "lex:ListImports",
    "lex:ListIntents",
    "lex:ListRecommendedIntents",
    "lex:ListSlots",
    "lex:ListSlotTypes",
    "lex:ListTagsForResource",
    "lex:SearchAssociatedTranscripts",
    "lex:ListCustomVocabularyItems"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLexReplicationPolicy

AmazonLexReplicationPolicy est une [politique AWS gérée](#) qui : autorise Amazon Lex à répliquer les ressources Lex entre les régions en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 31 janvier 2024, 23h29 UTC
- Heure modifiée : 8 mars 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
```

```
"lex:ListBotLocales",
"lex:CreateBotAlias",
"lex:UpdateBotAlias",
"lex>DeleteBotAlias",
"lex:DescribeBotAlias",
"lex:CreateBotVersion",
"lex>DeleteBotVersion",
"lex:DescribeBotVersion",
"lex:CreateExport",
"lex:DescribeBot",
"lex:UpdateExport",
"lex:DescribeExport",
"lex:DescribeBotLocale",
"lex:DescribeIntent",
"lex:ListIntents",
"lex:DescribeSlotType",
"lex:ListSlotTypes",
"lex:DescribeSlot",
"lex:ListSlots",
"lex:DescribeCustomVocabulary",
"lex:StartImport",
"lex:DescribeImport",
"lex:CreateBot",
"lex:UpdateBot",
"lex>DeleteBot",
"lex:CreateBotLocale",
"lex:UpdateBotLocale",
"lex>DeleteBotLocale",
"lex:CreateIntent",
"lex:UpdateIntent",
"lex>DeleteIntent",
"lex:CreateSlotType",
"lex:UpdateSlotType",
"lex>DeleteSlotType",
"lex:CreateSlot",
"lex:UpdateSlot",
"lex>DeleteSlot",
"lex:CreateCustomVocabulary",
"lex:UpdateCustomVocabulary",
"lex>DeleteCustomVocabulary",
"lex>DeleteBotChannel",
"lex>DeleteResourcePolicy"
],
"Resource" : [
```

```

    "arn:aws:lex:*:*:bot/*",
    "arn:aws:lex:*:*:bot-alias/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "ReplicationServicePolicyStatement2",
  "Effect" : "Allow",
  "Action" : [
    "lex:CreateUploadUrl",
    "lex:ListBots"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "ReplicationServicePolicyStatement3",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lexv2.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonLexRunBotsOnly

AmazonLexRunBotsOnly est une [politique AWS gérée](#) qui : Fournit un accès aux API conversationnelles Amazon Lex.

Utilisation de cette stratégie

Vous pouvez AmazonLexRunBotsOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:06 UTC
- Heure modifiée : 18 août 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex>DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ]
    }
  ]
}
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLexV2BotPolicy

AmazonLexV2BotPolicyest une [politiqueAWS gérée](#) qui : Permet aux robots Lex V2 d'accéder à d'autresAWS services en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 janvier 2021, 20:10 UTC
- Heure modifiée : 13 janvier 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AmazonLookoutEquipmentFullAccess

AmazonLookoutEquipmentFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet aux opérations d'Amazon Lookout for Equipment

Utilisation de cette stratégie

Vous pouvez AmazonLookoutEquipmentFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 avril 2021, 15:52 UTC
- Heure modifiée : 24 novembre 2021, 21 h 00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutEquipmentReadOnlyAccess

AmazonLookoutEquipmentReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Lookout for Equipments

Utilisation de cette stratégie

Vous pouvez AmazonLookoutEquipmentReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 5 mai 2021, 16:47 UTC
- Heure modifiée : 10 novembre 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutMetricsFullAccess

AmazonLookoutMetricsFullAccess est une [politique AWS gérée](#) qui : Donne accès à toutes les actions d'Amazon Lookout for Metrics

Utilisation de cette stratégie

Vous pouvez `AmazonLookoutMetricsFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 mai 2021, 00:43 UTC
- Heure modifiée : 7 mai 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
```

```
    "StringEquals" : {
      "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutMetricsReadOnlyAccess

AmazonLookoutMetricsReadOnlyAccess est une [politique AWS gérée](#) qui : Donne accès à toutes les actions en lecture seule pour Amazon Lookout for Metrics

Utilisation de cette stratégie

Vous pouvez AmazonLookoutMetricsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 mai 2021, 00:43 UTC
- Heure modifiée : 4 janvier 2022, 18:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutVisionConsoleFullAccess

AmazonLookoutVisionConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Lookout for Vision et un accès limité aux dépendances de service et de console requises.

Utilisation de cette stratégie

Vous pouvez les associer AmazonLookoutVisionConsoleFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 mai 2021, 19:37 UTC
- Heure modifiée : 11 mai 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3:PutLifecycleConfiguration",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketVersioning"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*"
},
{
  "Sid" : "LookoutVisionConsoleS3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*/*"
},
{
  "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
```

```
    "Effect" : "Allow",
    "Action" : [
      "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
      "groundtruthlabeling:AssociatePatchToManifestJob",
      "groundtruthlabeling:DescribeConsoleJob"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleDashboardAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleTagSelectorAccess",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetTagKeys",
      "tag:GetTagValues"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListAliases"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutVisionConsoleReadOnlyAccess

AmazonLookoutVisionConsoleReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon Lookout for Vision et un accès limité aux dépendances de service et de console requises.

Utilisation de cette stratégie

Vous pouvez AmazonLookoutVisionConsoleReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 mai 2021, 19:32 UTC
- Heure modifiée : 09 décembre 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
```

```

    "lookoutvision:DescribeProject",
    "lookoutvision:DescribeTrialDetection",
    "lookoutvision:DescribeModelPackagingJob",
    "lookoutvision:ListDatasetEntries",
    "lookoutvision:ListModels",
    "lookoutvision:ListProjects",
    "lookoutvision:ListTagsForResource",
    "lookoutvision:ListTrialDetections",
    "lookoutvision:ListModelPackagingJobs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*/*"
},
{
  "Sid" : "LookoutVisionConsoleDashboardAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon Lookout for Vision et un accès limité aux dépendances requises.

Utilisation de cette stratégie

Vous pouvez AmazonLookoutVisionFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 mai 2021, 19:24 UTC
- Heure modifiée : 11 mai 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Sid" : "LookoutVisionFullAccess",
    "Effect" : "Allow",
    "Action" : [
        "lookoutvision:*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonLookoutVisionReadOnlyAccess

AmazonLookoutVisionReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon Lookout for Vision et un accès limité aux dépendances requises.

Utilisation de cette stratégie

Vous pouvez AmazonLookoutVisionReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 mai 2021, 19:11 UTC
- Heure modifiée : 09 décembre 2021, 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningBatchPredictionsAccess

AmazonMachineLearningBatchPredictionsAccess est une [politique AWS gérée](#) qui : autorise les utilisateurs à demander des prédictions par lots à Amazon Machine Learning.

Utilisation de cette stratégie

Vous pouvez `AmazonMachineLearningBatchPredictionsAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 avril 2015, 17:12 UTC
- Heure modifiée : 9 avril 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningCreateOnlyAccess

AmazonMachineLearningCreateOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès de création à des ressources Amazon Machine Learning non prédictives.

Utilisation de cette stratégie

Vous pouvez AmazonMachineLearningCreateOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 avril 2015, 17:18 UTC
- Heure modifiée : 29 juin 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "machinelearning:Add*",
      "machinelearning:Create*",
      "machinelearning>Delete*",
      "machinelearning:Describe*",
      "machinelearning:Get*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningFullAccess

AmazonMachineLearningFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux ressources Amazon Machine Learning.

Utilisation de cette stratégie

Vous pouvez AmazonMachineLearningFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 avril 2015, 17:25 UTC
- Heure modifiée : 9 avril 2015, 17:25 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

AmazonMachineLearningManageRealTimeEndpointOnlyAccess est une [politiqueAWS gérée](#) qui : autorise les utilisateurs à créer et à supprimer le point de terminaison en temps réel pour les modèles Amazon Machine Learning.

Utilisation de cette stratégie

Vous pouvez `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 avril 2015, 17:32 UTC
- Heure modifiée : 9 avril 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningReadOnlyAccess

AmazonMachineLearningReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule aux ressources Amazon Machine Learning.

Utilisation de cette stratégie

Vous pouvez AmazonMachineLearningReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 avril 2015, 17:40 UTC
- Heure modifiée : 09 avril 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

AmazonMachineLearningRealTimePredictionOnlyAccess est une [politiqueAWS gérée](#) qui : autorise les utilisateurs à demander des prévisions en temps réel à Amazon Machine Learning.

Utilisation de cette stratégie

Vous pouvez AmazonMachineLearningRealTimePredictionOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 avril 2015, 17:44 UTC
- Heure modifiée : 9 avril 2015, 17:44 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonMachineLearningRealTimePredictionOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

AmazonMachineLearningRoleforRedshiftDataSourceV3 est une [politique AWS gérée](#) qui : Permet à Machine Learning de configurer et d'utiliser vos clusters Redshift et vos emplacements intermédiaires S3 pour la source de données Redshift.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonMachineLearningRoleforRedshiftDataSourceV3` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 24 juin 2020, 18h00 UTC
- Heure modifiée : 24 juin 2020, 18 h 00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutBucketPolicy",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy",
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::amazon-machine-learning*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMacieFullAccess

AmazonMacieFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Macie.

Utilisation de cette stratégie

Vous pouvez AmazonMacieFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 août 2017, 14:54 UTC
- Heure modifiée : 1 juillet 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMacieHandshakeRole

AmazonMacieHandshakeRole est une [politiqueAWS gérée](#) qui : accorde l'autorisation de créer le rôle lié à un service d'Amazon Macie.

Utilisation de cette stratégie

Vous pouvez AmazonMacieHandshakeRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 28 juin 2018, 15:46 UTC
- Heure modifiée : 28 juin 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AWSServiceName" : "macie.amazonaws.com"
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMacieReadOnlyAccess

AmazonMacieReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Macie.

Utilisation de cette politique

Vous pouvez l'associer AmazonMacieReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 juin 2023, 21:50 UTC
- Heure modifiée : 15 juin 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AmazonMacieServiceRole

AmazonMacieServiceRole est une [politique AWS gérée](#) qui : accorde à Macie un accès en lecture seule aux dépendances des ressources de votre compte afin de permettre l'analyse des données.

Utilisation de cette stratégie

Vous pouvez AmazonMacieServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 août 2017, 14:53 UTC
- Heure modifiée : 14 août 2017, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy est une [politique AWS gérée](#) qui : Rôle lié au service pour Amazon Macie

des politiques

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, groupes ou rôles.

détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 juin 2018
- Heure modifiée : 19 mai 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par politique est celle qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",

```



```
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectTagging"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
  ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées gérées et évoluez vers les autorisations gérées et évoluez vers les autorisations gérées](#)

AmazonManagedBlockchainConsoleFullAccess

AmazonManagedBlockchainConsoleFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à la chaîne de Amazon Managed Blockchain viaAWS Management Console

Utilisation de cette stratégie

Vous pouvezAmazonManagedBlockchainConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 avril 2019, 21:23 UTC
- Heure modifiée : 29 avril 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Effect" : "Allow",
"Action" : [
  "managedblockchain:*",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcs",
  "ec2:CreateVpcEndpoint",
  "kms:ListAliases",
  "kms:DescribeKey"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à la chaîne de Amazon Managed Blockchain.

Utilisation de cette stratégie

Vous pouvez les associer AmazonManagedBlockchainFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 avril 2019, 21:39 UTC
- Heure modifiée : 29 avril 2019, 21:39 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonManagedBlockchainReadOnlyAccess

AmazonManagedBlockchainReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à la chaîne de Amazon Managed Blockchain.

Utilisation de cette stratégie

Vous pouvez associer `AmazonManagedBlockchainReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : politiqueAWS gérée
- Heure de création : 30 avril 2019, 18:17 UTC
- Heure modifiée : 30 avril 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicyest une [politiqueAWS gérée](#) qui : Autorise l'accèsServices AWS aux ressources utilisées ou gérées par Amazon Managed Blockchain

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 janvier 2020, 19:51 UTC
- Heure modifiée : 17 janvier 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMCSFullAccess

AmazonMCSFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet au service Apache Cassandra géré par Amazon

Utilisation de cette stratégie

Vous pouvez AmazonMCSFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 13:45 UTC

- Heure modifiée : 17 avril 2020, 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling>DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```



```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMCSReadOnlyAccess

AmazonMCSReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule au service Apache Cassandra géré par Amazon

Utilisation de cette stratégie

Vous pouvez AmazonMCSReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 13:46 UTC

- Heure modifiée : 17 avril 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMechanicalTurkFullAccess

AmazonMechanicalTurkFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à toutes les API d'Amazon Mechanical Turk.

Utilisation de cette stratégie

Vous pouvez AmazonMechanicalTurkFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 décembre 2015, 19:08 UTC
- Heure modifiée : 11 décembre 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMechanicalTurkReadOnly

AmazonMechanicalTurkReadOnly est une [politique AWS gérée](#) qui : fournit un accès aux API en lecture seule dans Amazon Mechanical Turk.

Utilisation de cette stratégie

Vous pouvez AmazonMechanicalTurkReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 décembre 2015, 19:08 UTC
- Heure modifiée : 25 septembre 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMemoryDBFullAccess

AmazonMemoryDBFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon MemoryDB via le AWS Management Console.

Utilisation de la présente stratégie

Vous pouvez AmazonMemoryDBFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 octobre 2021, 19:24 UTC
- Heure modifiée : 8 octobre 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMemoryDBReadOnlyAccess

AmazonMemoryDBReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon MemoryDB via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonMemoryDBReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 octobre 2021, 19:27 UTC
- Heure modifiée : 8 octobre 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "memorydb:Describe*",
      "memorydb:List*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMobileAnalyticsFinancialReportAccess

AmazonMobileAnalyticsFinancialReportAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à tous les rapports, y compris les données financières pour toutes les ressources des applications.

Utilisation de cette stratégie

Vous pouvez AmazonMobileAnalyticsFinancialReportAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les ressources de l'application.

Utilisation de cette stratégie

Vous pouvez `AmazonMobileAnalyticsFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMobileAnalyticsNon-financialReportAccess

AmazonMobileAnalyticsNon-financialReportAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux rapports non financiers pour toutes les ressources de l'application.

Utilisation de cette stratégie

Vous pouvez AmazonMobileAnalyticsNon-financialReportAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : "mobileanalytics:GetReports",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMobileAnalyticsWriteOnlyAccess

AmazonMobileAnalyticsWriteOnlyAccess est une [stratégieAWS gérée](#) qui Donne uniquement l'accès d'écriture pour placer les données d'événements pour toutes les ressources d'application. (Recommandé pour l'intégration du SDK)

Utilisation de cette politique

Vous pouvezAmazonMobileAnalyticsWriteOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut d'une stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMonitronFullAccess

AmazonMonitronFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à la gestion d'Amazon Monitron

Utilisation de cette stratégie

Vous pouvez AmazonMonitronFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 décembre 2020, 22h40 UTC
- Heure modifiée : 8 juin 2022, 16:27 UTC

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

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```

    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "monitron.*.amazonaws.com"
        ]
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      }
    }
  },
  {
    "Sid" : "AWSSSOPermissions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "ds:DescribeDirectories",
      "ds:DescribeTrusts"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:DescribeStream",
      "kinesis:ListStreams"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents",
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMQApiFullAccess

AmazonMQApiFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à AmazonMQ via notre API/SDK.

Utilisation de cette stratégie

Vous pouvez AmazonMQApiFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 décembre 2018, 20:31 UTC
- Heure modifiée : 4 novembre 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "mq:*",
      "ec2:CreateNetworkInterface",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DetachNetworkInterface",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfacePermissions",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
    ]
  },
  {
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "mq.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMQApiReadOnlyAccess

AmazonMQApiReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à AmazonMQ via notre API/SDK.

Utilisation de cette stratégie

Vous pouvez AmazonMQApiReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 décembre 2018, 20:31 UTC
- Heure modifiée : 18 décembre 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Action" : [
      "mq:Describe*",
      "mq:List*",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMQFullAccess

AmazonMQFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à AmazonMQ via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonMQFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 novembre 2017, 15:28 UTC
- Heure modifiée : 4 novembre 2020, 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMQReadOnlyAccess

AmazonMQReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à AmazonMQ via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonMQReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 novembre 2017, 15h30 UTC
- Heure modifiée : 28 novembre 2017, 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicyest une [politiqueAWS gérée qui : Politique](#) en matière de rôles liés aux services pourAWS Amazon MQ

Utilisation cette politique politique politique politique.

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les utilisateurs, les rôles.

Les détails politique politique politique

- Type : Politique de rôles liée à un service
- Heure de création : 04 novembre 2020 novembre 2020, 16:07 novembre 2020 novembre 2020 novembre 2020, 16:07 novembre 2020
- Heure modifiée : 4 novembre 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La politique est celle qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
```

```
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AMQManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AMQManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
```



```
"Action" : [
  "logs:PutLogEvents",
  "logs:DescribeLogStreams",
  "logs:DescribeLogGroups",
  "logs:CreateLogStream",
  "logs:CreateLogGroup"
],
"Resource" : [
  "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon MSK Connect

Utilisation de cette stratégie

Vous pouvez AmazonMSKConnectReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 septembre 2021, 10:18 UTC
- Heure modifiée : 18 octobre 2021, 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "kafkaconnect:DescribeWorkerConfiguration"
  ],
  "Resource" : [
    "arn:aws:kafkaconnect:*:*:worker-configuration/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMSKFullAccess

AmazonMSKFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon MSK et les autres autorisations requises pour ses dépendances.

Utilisation de cette politique

Vous pouvez vous associer AmazonMSKFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 janvier 2019, 22:07 UTC
- Heure modifiée : 18 octobre 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "aws:RequestTag/ClusterArn" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "ec2:ResourceTag/ClusterArn" : "*"
    }
  }
}
```

```

    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "kafka.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "kafka.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon MSK

Utilisation de cette stratégie

Vous pouvez les associer AmazonMSKReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 14 janvier 2019, 22:28 UTC
- Heure modifiée : 14 janvier 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonMWAAServiceRolePolicy

AmazonMWAAServiceRolePolicy est une [politiqueAWS gérée](#) qui : Le rôle lié au service utilisé par Amazon Managed Workflows pour Apache Airflow.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 24 novembre 2020, 14:13 UTC
- Heure modifiée : 17 novembre 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonMWAAManaged" : false
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "AmazonMWAAManaged"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/MWAA"
        ]
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker est une [politique AWS gérée](#) qui : Cette politique donne accès aux ressources nécessaires aux utilisateurs de Nimble Studio Launch Profile. Attachez cette politique aux instances EC2 créées par Nimble Studio Builder.

Utilisation de cette stratégie

Vous pouvez AmazonNimbleStudio-LaunchProfileWorker les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:47 UTC
- Heure modifiée : 28 avril 2021, 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin est une [politique AWS gérée](#) qui : Cette politique accorde l'accès aux ressources Amazon Nimble Studio associées à l'administrateur du studio et aux ressources de studio associées dans d'autres services. Associez cette politique au rôle d'administrateur associé à votre studio.

Utilisation de cette politique

Vous pouvez vous associer AmazonNimbleStudio-StudioAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:47 UTC
- Heure modifiée : 22 septembre 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
```

```

    "nimble:CreateStreamingSessionStream",
    "nimble:GetStreamingSessionStream",
    "nimble>DeleteStreamingSession",
    "nimble:ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup",
    "nimble:ListEulas",
    "nimble:ListEulaAcceptances",
    "nimble:GetEula",
    "nimble:AcceptEulas",
    "nimble:ListStudioMembers",
    "nimble:GetStudioMember",
    "nimble:ListStreamingSessions",
    "nimble:GetStreamingImage",
    "nimble:ListStreamingImages",
    "nimble:GetLaunchProfileInitialization",
    "nimble:GetLaunchProfileDetails",
    "nimble:GetFeatureMap",
    "nimble:PutStudioLogEvents",
    "nimble:ListLaunchProfiles",
    "nimble:GetLaunchProfile",
    "nimble:GetLaunchProfileMember",
    "nimble:ListLaunchProfileMembers",
    "nimble:PutLaunchProfileMembers",
    "nimble:UpdateLaunchProfileMember",
    "nimble>DeleteLaunchProfileMember"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers",
    "identitystore:DescribeUser",
    "identitystore:ListUsers"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",

```

```
    "ds:DescribeDirectories",
    "ec2:DescribeSubnets",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2>DeleteNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeSecurityGroups",
    "fsx:DescribeFileSystems"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "nimble.amazonaws.com"
    }
  }
},
"Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonNimbleStudio-StudioUser

AmazonNimbleStudio-StudioUser est une [politique AWS gérée](#) qui : Cette politique accorde l'accès aux ressources Amazon Nimble Studio associées à l'utilisateur du studio et aux ressources de studio associées dans d'autres services. Associez cette politique au rôle d'utilisateur associé à votre studio.

Utilisation de cette politique

Vous pouvez vous associer `AmazonNimbleStudio-StudioUser` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:48 UTC
- Heure modifiée : 22 septembre 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```



```
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "nimble.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sso-directory:DescribeUsers",
      "sso-directory:SearchUsers",
      "identitystore:DescribeUser",
      "identitystore:ListUsers"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "nimble:ListLaunchProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "nimble:requesterPrincipalId" : "${nimble:principalId}"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "nimble:ListStudioMembers",
      "nimble:GetStudioMember",
      "nimble:ListEulas",
      "nimble:ListEulaAcceptances",
      "nimble:GetFeatureMap",
      "nimble:PutStudioLogEvents"
    ],
    "Resource" : "*"
  },
  {
```

```
"Effect" : "Allow",
"Action" : [
  "nimble:DeleteStreamingSession",
  "nimble:GetStreamingSession",
  "nimble:StartStreamingSession",
  "nimble:StopStreamingSession",
  "nimble>CreateStreamingSessionStream",
  "nimble:GetStreamingSessionStream",
  "nimble:ListStreamingSessions",
  "nimble:ListStreamingSessionBackups",
  "nimble:GetStreamingSessionBackup"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
  }
}
},
"Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonOmicsFullAccess

AmazonOmicsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Omics et aux autres fonctionnalités requises Services AWS. Cette politique permet à l'utilisateur de consulter et d'accepter les invitations à partager de la RAM pour accéder à des ressources extérieures à celles de l'utilisateur Compte AWS.

Utilisation de cette stratégie

Vous pouvez AmazonOmicsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 février 2023, 00:59 UTC
- Heure modifiée : 24 février 2023, 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "omics.amazonaws.com"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOmicsReadOnlyAccess

AmazonOmicsReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Omics

Utilisation de cette stratégie

Vous pouvez AmazonOmicsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2022, 04:17 UTC
- Heure modifiée : 29 novembre 2022, 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOneEnterpriseFullAccess

AmazonOneEnterpriseFullAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations administratives qui permettent d'accéder à toutes les ressources et opérations d'Amazon One Enterprise.

Utilisation de cette politique

Vous pouvez vous associer `AmazonOneEnterpriseFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 04:58 UTC
- Heure modifiée : 28 novembre 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonOneEnterpriseInstallerAccess

AmazonOneEnterpriseInstallerAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations de lecture et d'écriture limitées qui permettent l'installation et l'activation du terminal.

Utilisation de cette politique

Vous pouvez vous associer AmazonOneEnterpriseInstallerAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 05:00 UTC
- Heure modifiée : 28 novembre 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "one:CreateDeviceActivationQrCode",
  "one:GetDeviceInstance",
  "one:GetSite",
  "one:GetSiteAddress",
  "one:ListDeviceInstances",
  "one:ListSites"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonOneEnterpriseReadOnlyAccess

AmazonOneEnterpriseReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations de lecture seule à toutes les ressources et opérations Amazon One Enterprise.

Utilisation de cette politique

Vous pouvez vous associer AmazonOneEnterpriseReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 04:59 UTC
- Heure modifiée : 28 novembre 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonOpenSearchDashboardsServiceRolePolicy

AmazonOpenSearchDashboardsServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un accès au service Amazon OpenSearch Dashboards pour accéder à d'autres AWS services, par exemple en votre CloudWatch nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 22 décembre 2023, 19:38 UTC
- Heure modifiée : 22 décembre 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonOpenSearchIngestionFullAccess

AmazonOpenSearchIngestionFullAccess est une [politique AWS gérée](#) qui : autorise AmazonOpenSearch Ingestion à accéder à d'autres AWS services en votre nom.

Utilisation de cette stratégie

Vous pouvez AmazonOpenSearchIngestionFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 avril 2023, 18:11 UTC
- Heure modifiée : 26 avril 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "osis:CreatePipeline",
      "osis:UpdatePipeline",
      "osis>DeletePipeline",
      "osis:StartPipeline",
      "osis:StopPipeline",
      "osis>ListPipelines",
      "osis:GetPipeline",
      "osis:GetPipelineChangeProgress",
      "osis:ValidatePipeline",
      "osis:GetPipelineBlueprint",
      "osis>ListPipelineBlueprints",
      "osis:TagResource",
      "osis:UntagResource",
      "osis>ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "osis.amazonaws.com"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOpenSearchIngestionReadOnlyAccess

AmazonOpenSearchIngestionReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à AmazonOpenSearch Ingestion Service

Utilisation de cette stratégie

Vous pouvez AmazonOpenSearchIngestionReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 26 avril 2023, 18:09 UTC
- Heure modifiée : 26 avril 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",

```

```
        "osis:ListTagsForResource"  
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOpenSearchIngestionServiceRolePolicy

AmazonOpenSearchIngestionServiceRolePolicyest une [politiqueAWS gérée](#) qui : autorise Amazon OpenSearch Ingestion Service à accéder à d'autresAWS services en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à des rôles

des des des des des

- Type : Politique de rôles liée à un service
- Heure de création : 18 novembre 2022, 16:49 UTC
- Heure modifiée : 18 novembre 2022, 16:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La politique Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

de politique J

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWSdes stratégies](#)

AmazonOpenSearchServerlessServiceRolePolicy

AmazonOpenSearchServerlessServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon OpenSearch Serverless à accéder à d'autres AWS services tels que CloudWatch les API en votre nom.

Utilisation de cette politique de politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des utilisateurs, des groupes ou des rôles.

Détails des politiques des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 24 novembre 2022, 19:50 UTC
- Heure modifiée : 24 novembre 2022, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "cloudwatch:namespace" : "AWS/AOSS"  
    }  
  }  
} ]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège des privilèges des moins de privilège des autorisations de moindre privilège des](#)

AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess est une [politiqueAWS gérée](#) qui : fournit un accès au service de configuration Amazon Cognito.

Utilisation de cette stratégie

Vous pouvez AmazonOpenSearchServiceCognitoAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 2 septembre 2021, 06:31 UTC
- Heure modifiée : 20 décembre 2021, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp>DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam:*:*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOpenSearchServiceFullAccess

AmazonOpenSearchServiceFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet au OpenSearch service de configuration Amazon Service.

Utilisation de cette stratégie

Vous pouvez AmazonOpenSearchServiceFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 septembre 2021, 05:33 UTC
- Heure modifiée : 8 septembre 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOpenSearchServiceReadOnlyAccess

AmazonOpenSearchServiceReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule au OpenSearch service de configuration Amazon Service.

Utilisation de cette stratégie

Vous pouvez AmazonOpenSearchServiceReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 septembre 2021, 05:38 UTC
- Heure modifiée : 8 septembre 2021, 05:38 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonOpenSearchServiceRolePolicy

AmazonOpenSearchServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon OpenSearch Service à accéder à d'autres AWS services tels que les API réseau EC2 en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 26 août 2021, 09:27 UTC
- Heure modifiée : 23 octobre 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeNetworkInterfaces"
],
"Resource" : "*"
},
{
  "Sid" : "Stmt1480452973144",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ]
},
{
  "Sid" : "Stmt1480452973165",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Sid" : "Stmt1480452973149",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973150",
  "Effect" : "Allow",
  "Action" : [
    "ec2:UnAssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
```



```
"Sid" : "Stmt1480452973154",
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeSecurityGroups"
],
"Resource" : "*"
},
{
  "Sid" : "Stmt1480452973164",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973174",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973184",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddListenerCertificates",
    "elasticloadbalancing:RemoveListenerCertificates"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:listener/*"
  ]
},
{
  "Sid" : "Stmt1480452973194",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ]
},
}
```

```
{
  "Sid" : "Stmt1480452973195",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeTags"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973196",
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973197",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/ES"
    }
  }
},
{
  "Sid" : "Stmt1480452973198",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "Stmt1480452973199",
  "Effect" : "Allow",
```

```
"Action" : "ec2:CreateVpcEndpoint",
"Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/OpenSearchManaged" : "true"
  }
}
},
{
  "Sid" : "Stmt1480452973200",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/OpenSearchManaged" : "true"
    }
  }
},
{
  "Sid" : "Stmt1480452973201",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973202",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
}
]
```

```
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonPersonalizeFullAccess

AmazonPersonalizeFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Personalize via le SDK AWS Management Console and. Fournit également un accès sélectif aux services connexes (par exemple, S3, CloudWatch).

Utilisation de cette stratégie

Vous pouvez AmazonPersonalizeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 4 décembre 2018, 22:24 UTC
- Heure modifiée : 30 mai 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "personalize:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::*Personalize*",
      "arn:aws:s3:::*personalize*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "personalize.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPollyFullAccess

AmazonPollyFullAccess est une [politiqueAWS gérée](#) qui : accorde un accès complet au service et aux ressources Amazon Polly.

Utilisation de cette stratégie

Vous pouvez AmazonPollyFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 novembre 2016, 18:59 UTC
- Heure modifiée : 30 novembre 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "polly:*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPollyReadOnlyAccess

AmazonPollyReadOnlyAccess est une [politiqueAWS gérée](#) qui : Accorde un accès en lecture seule aux ressources Amazon Polly.

Utilisation de cette stratégie

Vous pouvez AmazonPollyReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 novembre 2016, 18:59 UTC
- Heure modifiée : 17 juillet 2018, 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPrometheusConsoleFullAccess

AmazonPrometheusConsoleFullAccess est une [politique AWS gérée](#) qui : Accorde un accès complet aux ressources Prometheus AWS gérées dans la AWS console

Utilisation de cette stratégie

Vous pouvez `AmazonPrometheusConsoleFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 18:11 UTC
- Heure modifiée : 24 octobre 2022, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
```

```
    "aps:DeleteWorkspace",
    "aps:ListWorkspaces",
    "aps:DescribeAlertManagerDefinition",
    "aps:DescribeRuleGroupsNamespace",
    "aps:CreateAlertManagerDefinition",
    "aps:CreateRuleGroupsNamespace",
    "aps>DeleteAlertManagerDefinition",
    "aps>DeleteRuleGroupsNamespace",
    "aps>ListRuleGroupsNamespaces",
    "aps:PutAlertManagerDefinition",
    "aps:PutRuleGroupsNamespace",
    "aps:TagResource",
    "aps:UntagResource",
    "aps>CreateLoggingConfiguration",
    "aps:UpdateLoggingConfiguration",
    "aps>DeleteLoggingConfiguration",
    "aps:DescribeLoggingConfiguration"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPrometheusFullAccess

AmazonPrometheusFullAccess est une [politique AWS gérée](#) qui : accorde un accès complet aux ressources AWS gérées de Prometheus

Utilisation de cette politique

Vous pouvez vous associer AmazonPrometheusFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 18:10 UTC
- Heure modifiée : 26 novembre 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
},
"Resource" : "*"
},
{
  "Sid" : "CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScrapper*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonPrometheusQueryAccess

AmazonPrometheusQueryAccess est une [politique AWS gérée](#) qui : Autorise l'accès à l'exécution de requêtes sur les ressources PrometheusAWS gérées

Utilisation de cette stratégie

Vous pouvez AmazonPrometheusQueryAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 19 décembre 2020, 01:02 UTC
- Heure modifiée : 19 décembre 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPrometheusRemoteWriteAccess

AmazonPrometheusRemoteWriteAccess est une [politiqueAWS gérée](#) qui : Accorde uniquement l'accès en écriture aux espaces de travail PrometheusAWS gérés

Utilisation de cette stratégie

Vous pouvez AmazonPrometheusRemoteWriteAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 19 décembre 2020, 01:04 UTC
- Heure modifiée : 19 décembre 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonPrometheusScrapperServiceRolePolicy

AmazonPrometheusScrapperServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un accès aux AWS ressources gérées ou utilisées par Amazon Managed Service pour Prometheus Collector

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 26 novembre 2023, 14:19 UTC
- Heure modifiée : 26 novembre 2023, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "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:*:ec2:*:*:network-interface/*",
      "Condition" : {
```



```
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "Null" : {
      "aws:RequestTag/AMPAgentlessScrapper" : "false"
    }
  }
},
{
  "Sid" : "ENIUpdating",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AMPAgentlessScrapper" : "false"
    }
  }
},
{
  "Sid" : "EKSAccess",
  "Effect" : "Allow",
  "Action" : "eks:DescribeCluster",
  "Resource" : "arn:*:eks:*:*:cluster/*"
},
{
  "Sid" : "APSWriting",
  "Effect" : "Allow",
  "Action" : "aps:RemoteWrite",
  "Resource" : "arn:*:aps:*:*:workspace/*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonQFullAccess

AmazonQFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet pour permettre les interactions avec Amazon Q

Utilisation de cette politique

Vous pouvez vous associer AmazonQFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 16h00 UTC
- Heure modifiée : 28 novembre 2023, 16h00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonQLDBConsoleFullAccess

AmazonQLDBConsoleFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon QLDB via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonQLDBConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 5 septembre 2019, 18:24 UTC
- Heure modifiée : 4 novembre 2022, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb>DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dbqms:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:ListStreams",
      "kinesis:DescribeStream"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "qldb.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonQLDBFullAccess

AmazonQLDBFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon QLDB via l'API du service.

Utilisation de cette stratégie

Vous pouvez AmazonQLDBFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 5 septembre 2019, 18:23 UTC
- Heure modifiée : 4 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb>DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",

```

```

    "qldb:ListJournalS3ExportsForLedger",
    "qldb:DescribeJournalS3Export",
    "qldb:CancelJournalKinesisStream",
    "qldb:DescribeJournalKinesisStream",
    "qldb:ListJournalKinesisStreamsForLedger",
    "qldb:StreamJournalToKinesis",
    "qldb:GetDigest",
    "qldb:GetRevision",
    "qldb:GetBlock",
    "qldb:TagResource",
    "qldb:UntagResource",
    "qldb:ListTagsForResource",
    "qldb:SendCommand",
    "qldb:PartiQLCreateTable",
    "qldb:PartiQLCreateIndex",
    "qldb:PartiQLDropTable",
    "qldb:PartiQLDropIndex",
    "qldb:PartiQLUndropTable",
    "qldb:PartiQLDelete",
    "qldb:PartiQLInsert",
    "qldb:PartiQLUpdate",
    "qldb:PartiQLSelect",
    "qldb:PartiQLHistoryFunction",
    "qldb:PartiQLRedact"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "qldb.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonQLDBReadOnly

AmazonQLDBReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon QLDB.

Utilisation de cette stratégie

Vous pouvez AmazonQLDBReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 5 septembre 2019, 18:19 UTC
- Heure modifiée : 2 juillet 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
    "qldb:DescribeLedger",
    "qldb:ListJournalS3Exports",
    "qldb:ListJournalS3ExportsForLedger",
    "qldb:DescribeJournalS3Export",
    "qldb:DescribeJournalKinesisStream",
    "qldb:ListJournalKinesisStreamsForLedger",
    "qldb:GetBlock",
    "qldb:GetDigest",
    "qldb:GetRevision",
    "qldb:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRDSBetaServiceRolePolicy

AmazonRDSBetaServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à Amazon RDS de gérer les AWS ressources en votre nom.

Utilisation de cette politique politique de politique

Cette politique est attachée à un rôle lié à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 2 mai 2018, 19:41 UTC
- Heure modifiée : 14 décembre 2022, 18:33 UTC

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

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON stratégie I

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies gérées et évoluez vers les stratégies AWS gérées et évoluez vers les stratégies de moindre privilège et évoluez vers les](#)

AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicy est une [politique AWS gérée](#) qui : permet à Amazon RDS Custom d'effectuer diverses actions d'automatisation et tâches de gestion de base de données via un profil d'instance EC2.

Utilisation de cette politique

Vous pouvez vous associer AmazonRDSCustomInstanceProfileRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 février 2024, 17:42 UTC
- Heure modifiée : 27 février 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
```

```
    "ssm:GetDocument",
    "ssm:DescribeDocument"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/*"
},
{
  "Sid" : "ssmAgentPermission4",
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:OpenControlChannel"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ssmAgentPermission5",
  "Effect" : "Allow",
  "Action" : [
    "ec2messages:AcknowledgeMessage",
    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Sid" : "createEc2SnapshotPermission1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "createEc2SnapshotPermission2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createEc2SnapshotPermission3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*::instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createTagForEc2SnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
```



```

"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ],
    "ec2:CreateAction" : [
      "CreateSnapshot",
      "CreateSnapshots"
    ]
  }
},
{
  "Sid" : "rdsCustomS3ObjectPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:putObject",
    "s3:getObject",
    "s3:getObjectVersion",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : [
    "arn:aws:s3::do-not-delete-rds-custom-*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "rdsCustomS3BucketPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucketVersions",
    "s3:ListBucketMultipartUploads"
  ],
  "Resource" : [
    "arn:aws:s3::do-not-delete-rds-custom-*"
  ],

```

```
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
},
{
  "Sid" : "readSecretsFromCpPermission",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createSecretsOnDpPermission",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
    }
  }
},
{
  "Sid" : "publishCwMetricsPermission",
```

```

    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "rdscustom/rds-custom-sqlserver-agent",
          "RDSCustomForOracle/Agent"
        ]
      }
    }
  },
  {
    "Sid" : "putEventsToEventBusPermission",
    "Effect" : "Allow",
    "Action" : "events:PutEvents",
    "Resource" : "arn:aws:events:*:*:event-bus/default"
  },
  {
    "Sid" : "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"
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSCustomPreviewServiceRolePolicy

AmazonRDSCustomPreviewServiceRolePolicy est une [politique AWS gérée](#) qui : Amazon RDS Custom Preview Service Role Policy

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 08 octobre 2021, 21:44 UTC
- Heure modifiée : 20 septembre 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "ecc2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ecc1scoping",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AllocateAddress"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
}
```

```
  },
  {
    "Sid" : "ecc1scoping2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateAddress",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ecc1scoping3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances1",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
```



```

    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac",
        "custom-oracle"
      ]
    }
  }
}
}

```

```
  },
  {
    "Sid" : "RequireImdsV2",
    "Effect" : "Deny",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringNotEquals" : {
        "ec2:MetadataHttpTokens" : "required"
      },
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances3keyPair1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2>DeleteKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccKeyPair2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateKeyPair"
    ],
    "Resource" : [
```

```

    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccNetworkInterface1",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccNetworkInterface2",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group*"
  ]
},
{
  "Sid" : "eccNetworkInterface3",
  "Effect" : "Allow",
  "Action" : "ec2>DeleteNetworkInterface",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "eccCreateTag1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccCreateTag2",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ],
      "ec2:CreateAction" : [
        "CreateKeyPair",
        "RunInstances",
        "CreateNetworkInterface",
        "CreateVolume",
        "CreateSnapshots",
        "CopySnapshot",
        "AllocateAddress"
      ]
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "eccVolume1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVolume",
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
```

```
    "ec2:ModifyVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccVolume4snapshot1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume",
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopySnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
```

```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "eccSnapshot3",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshots",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "iam1",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:GetInstanceProfile",
      "iam:GetRole",
      "iam:ListRolePolicies",
      "iam:GetRolePolicy",
      "iam:ListAttachedRolePolicies",
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "iam2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/AWSRDSCustom*",
    "Condition" : {
```

```

    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  },
  {
    "Sid" : "cloudtrail1",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:GetTrailStatus"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "cw1",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:EnableAlarmActions",
      "cloudwatch:DeleteAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "cw2",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:TagResource"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",

```



```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "cw3",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
  },
  {
    "Sid" : "ssm1",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ssm:*:*:document/*"
  },
  {
    "Sid" : "ssm2",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ssm3",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetCommandInvocation",
      "ssm:GetConnectionStatus",
      "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
  },
  },
```

```
{
  "Sid" : "ssm4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ssm5",
  "Effect" : "Allow",
  "Action" : [
    "ssm>DeleteParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eb1",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:TagResource"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",

```

```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "eb2",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:DescribeRule",
      "events:EnableRule",
      "events:ListTargetsByRule",
      "events>DeleteRule",
      "events:RemoveTargets",
      "events:DisableRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eb3",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "events:ManagedBy" : [
          "custom.rds-preview.amazonaws.com"
        ]
      }
    }
  },
  {
```

```

    "Sid" : "eb4",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:EnableRule",
      "events>DeleteRule",
      "events:RemoveTargets",
      "events:DisableRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "events:ManagedBy" : [
          "custom.rds-preview.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "eb5",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "secretmanager1",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  }
}

```

```
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon RDS Custom à gérer les AWS ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 08 octobre 2021, 21:39 UTC
- Heure modifiée : 20 septembre 2023, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
```

```

    "ec2:RegisterImage",
    "ec2:DeregisterImage",
    "ec2:DescribeTags",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVolumesModifications",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:SearchTransitGatewayMulticastGroups",
    "ec2:GetTransitGatewayMulticastDomainAssociations",
    "ec2:DescribeTransitGatewayMulticastDomains",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ecc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation",
    "ec2:TerminateInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:RebootInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping",

```

```
"Effect" : "Allow",
"Action" : [
  "ec2:AllocateAddress"
],
"Resource" : [
  "*"
],
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ]
  }
}
},
{
  "Sid" : "ecc1scoping2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
},
{
  "Sid" : "ecc1scoping3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses"
  ],
```



```

    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances1",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
      "arn:aws:ec2:*:*:placement-group/*"
    ]
  },
  {
    "Sid" : "eccRunInstances3",

```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac",
          "custom-oracle"
        ]
      }
    }
  },
  {
    "Sid" : "RequireImdsV2",
    "Effect" : "Deny",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringNotEquals" : {
        "ec2:MetadataHttpTokens" : "required"
      },
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances3keyPair1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2>DeleteKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition" : {

```

```

    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "eccKeyPair2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccNetworkInterface1",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccNetworkInterface2",
    "Effect" : "Allow",

```

```

    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "eccNetworkInterface3",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccCreateTag1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccCreateTag2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "*",
    "Condition" : {

```

```
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ],
      "ec2:CreateAction" : [
        "CreateKeyPair",
        "RunInstances",
        "CreateNetworkInterface",
        "CreateVolume",
        "CreateSnapshot",
        "CreateSnapshots",
        "CopySnapshot",
        "AllocateAddress"
      ]
    }
  },
  {
    "Sid" : "eccVolume1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVolume",
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ]
  }
},
{
  "Sid" : "eccVolume3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVolumeAttribute",
    "ec2>DeleteVolume",
    "ec2:ModifyVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccVolume4snapshot1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume",
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Sid" : "eccSnapshot2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopySnapshot",
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot4",
  "Effect" : "Allow",
```

```
"Action" : "ec2:CreateSnapshot",
"Resource" : [
  "arn:aws:ec2:*:*:volume/*"
],
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/AWSRDSCustom" : [
      "custom-sqlserver"
    ]
  }
}
},
{
  "Sid" : "iam1",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:GetInstanceProfile",
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : "*"
},
{
  "Sid" : "iam2",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
}
},
{
  "Sid" : "cloudtrail1",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:GetTrailStatus"
  ],
}
```



```
    "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "cw1",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:EnableAlarmActions",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "cw2",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:TagResource"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "cw3",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms"
    ],
```

```
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
  },
  {
    "Sid" : "ssm1",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ssm:*:*:document/*"
  },
  {
    "Sid" : "ssm2",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ssm3",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetCommandInvocation",
      "ssm:GetConnectionStatus",
      "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ssm4",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter",
      "ssm:AddTagsToResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
```

```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "ssm5",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DeleteParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eb1",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:TagResource"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eb2",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:DescribeRule",
```

```
    "events:EnableRule",
    "events:ListTargetsByRule",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eb3",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "events:ManagedBy" : [
        "custom.rds.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "eb4",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:EnableRule",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
```

```
    "StringLike" : {
      "events:ManagedBy" : [
        "custom.rds.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "eb5",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "secretmanager1",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "secretmanager2",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*,
```

```
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ]
  }
},
{
  "Sid" : "sqs1",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs:TagQueue"
  ],
  "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-sqlserver"
      ]
    }
  }
},
{
  "Sid" : "sqs2",
  "Effect" : "Allow",
  "Action" : [
    "sqs:GetQueueAttributes",
    "sqs:SendMessage",
    "sqs:ReceiveMessage",
    "sqs>DeleteMessage",
    "sqs>DeleteQueue"
  ],
  "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-sqlserver"
      ]
    }
  }
}
```

```
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSDDataFullAccess

AmazonRDSDDataFullAccess est une [politique AWS gérée](#) qui : autorise un accès complet à l'utilisation des API de données RDS, des API de stockage secret pour les informations d'identification de la base de données RDS et des API de gestion des requêtes de la console de base de données pour exécuter des instructions SQL sur des clusters Aurora Serverless dans le Compte AWS.

Utilisation de cette stratégie

Vous pouvez les associer AmazonRDSDDataFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 novembre 2018, 21:29 UTC
- Heure modifiée : 20 novembre 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDDataFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms>DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms>DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",

```



```
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRDSDirectoryServiceAccess

AmazonRDSDirectoryServiceAccess est une [politique AWS gérée](#) qui : autorise RDS à accéder à Directory Service Managed AD pour le compte du client pour les instances de base de données SQL Server jointes à un domaine.

Utilisation de cette stratégie

Vous pouvez AmazonRDSDirectoryServiceAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 26 février 2016, 02:02 UTC
- Heure modifiée : 15 mai 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRDSEnhancedMonitoringRole

AmazonRDSEnhancedMonitoringRole est une [politique AWS gérée](#) qui : Fournit un accès à Cloudwatch for RDS Enhanced Monitoring

Utilisation de cette stratégie

Vous pouvez les associer `AmazonRDSEnhancedMonitoringRole` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 novembre 2015, 19:58 UTC
- Heure modifiée : 11 novembre 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
```

```
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRDSFullAccess

AmazonRDSFullAccess est un [AWS politique gérée](#) qui : fournit un accès complet à Amazon RDS via le AWS Management Console.

Utilisation de cette politique

Vous pouvez joindre AmazonRDSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 06 février 2015, 18:40 UTC
- Heure modifiée : 17 août 2023, 23h00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
```

```

    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "outposts:GetOutpostInstanceTypes",
    "devops-guru:GetResourceCollection"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "pi:*",
  "Resource" : [
    "arn:aws:pi:*:*:metrics/rds/*",
    "arn:aws:pi:*:*:perf-reports/rds/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "rds.amazonaws.com",
        "rds.application-autoscaling.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "devops-guru:SearchInsights",
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [
        "RDS"
      ]
    }
  },
  "Null" : {
    "devops-guru:ServiceNames" : "false"
  }
}

```

```
}  
  }  
] }  
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AmazonRDSPerformanceInsightsFullAccess

AmazonRDSPerformanceInsightsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à RDS Performance Insights via AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonRDSPerformanceInsightsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 août 2023, 23:41 UTC
- Heure modifiée : 23 octobre 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi>CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi>DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
```



```
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonCloudWatchReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSPerformanceInsightsReadOnly

AmazonRDSPerformanceInsightsReadOnly est une [politique AWS gérée qui : politique](#) en lecture seule pour RDS Performance Insights

Utilisation de cette politique

Vous pouvez vous associer AmazonRDSPerformanceInsightsReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 avril 2022, 00:02 UTC

- Heure modifiée : 23 octobre 2023, 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
```

```

    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetadata",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceDimensions",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
    "Effect" : "Allow",
    "Action" : "pi:GetPerformanceAnalysisReport",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
    "Effect" : "Allow",
    "Action" : "pi:ListPerformanceAnalysisReports",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
    "Effect" : "Allow",
    "Action" : "pi:ListTagsForResource",
    "Resource" : "arn:aws:pi:*:*:*/rds/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy est une [politique AWS gérée](#) qui : Amazon RDS Preview Service Role Policy

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 31 mai 2018, 18:02 UTC
- Heure modifiée : 4 octobre 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "rds:CrossRegionCommunication"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateCoipPoolPermission",
      "ec2:CreateLocalGatewayRouteTablePermission",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteCoipPoolPermission",
      "ec2>DeleteLocalGatewayRouteTablePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeCoipPools",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeLocalGatewayRouteTablePermissions",
      "ec2:DescribeLocalGatewayRouteTables",
      "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
      "ec2:DescribeLocalGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcs",
      "ec2:DisassociateAddress",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:ReleaseAddress",
      "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
    "sns:Publish"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/DocDB-Preview",
        "AWS/Neptune-Preview",
        "AWS/RDS-Preview",
        "AWS/Usage"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```

    "secretsmanager:GetRandomPassword"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DeleteSecret",
    "secretsmanager:DescribeSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:RotateSecret",
    "secretsmanager:UpdateSecret",
    "secretsmanager:UpdateSecretVersionStage",
    "secretsmanager:ListSecretVersionIds"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
  ],
  "Condition" : {
    "StringLike" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "secretsmanager:TagResource",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws:rds:primaryDBInstanceArn",
        "aws:rds:primaryDBClusterArn"
      ]
    },
    "StringLike" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
    }
  }
}
]

```

```
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon RDS via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonRDSReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 14 avril 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
"Action" : [
  "rds:Describe*",
  "rds:ListTagsForResource",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeInternetGateways",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcAttribute",
  "ec2:DescribeVpcs"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "devops-guru:GetResourceCollection"
  ],
  "Resource" : "*"
},
{
  "Action" : [
    "devops-guru:SearchInsights",
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [
        "RDS"
      ]
    },
    "Null" : {
      "devops-guru:ServiceNames" : "false"
    }
  }
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRDSServiceRolePolicy

AmazonRDSServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon RDS à gérer les AWS ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 08 janvier 2018, 18:17 UTC
- Heure modifiée : 19 janvier 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CrossRegionCommunication",
    "Effect" : "Allow",
    "Action" : [
      "rds:CrossRegionCommunication"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Ec2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateCoipPoolPermission",
      "ec2:CreateLocalGatewayRouteTablePermission",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteCoipPoolPermission",
      "ec2>DeleteLocalGatewayRouteTablePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeCoipPools",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeLocalGatewayRouteTablePermissions",
      "ec2:DescribeLocalGatewayRouteTables",
      "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
      "ec2:DescribeLocalGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcs",
      "ec2:DisassociateAddress",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:ModifyVpcEndpoint",
      "ec2:ReleaseAddress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateVpcEndpoint",
      "ec2:DescribeVpcEndpoints",
```

```

    "ec2:DeleteVpcEndpoints",
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Sns",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*",
    "arn:aws:logs:*:*:log-group:/aws/docdb/*",
    "arn:aws:logs:*:*:log-group:/aws/neptune*"
  ]
},
{
  "Sid" : "CloudWatchStreams",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
  ]
},
{
  "Sid" : "Kinesis",
  "Effect" : "Allow",
  "Action" : [

```

```

    "kinesis:CreateStream",
    "kinesis:PutRecord",
    "kinesis:PutRecords",
    "kinesis:DescribeStream",
    "kinesis:SplitShard",
    "kinesis:MergeShards",
    "kinesis>DeleteStream",
    "kinesis:UpdateShardCount"
  ],
  "Resource" : [
    "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
  ]
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/DocDB",
        "AWS/Neptune",
        "AWS/RDS",
        "AWS/Usage"
      ]
    }
  }
},
{
  "Sid" : "SecretsManagerPassword",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerSecret",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager>DeleteSecret",

```

```

    "secretsmanager:DescribeSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:RotateSecret",
    "secretsmanager:UpdateSecret",
    "secretsmanager:UpdateSecretVersionStage",
    "secretsmanager:ListSecretVersionIds"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:rds!*"
  ],
  "Condition" : {
    "StringLike" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
    }
  }
},
{
  "Sid" : "SecretsManagerTags",
  "Effect" : "Allow",
  "Action" : "secretsmanager:TagResource",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws:rds:primaryDBInstanceArn",
        "aws:rds:primaryDBClusterArn"
      ]
    },
    "StringLike" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftAllCommandsFullAccess

AmazonRedshiftAllCommandsFullAccess est une [politique AWS gérée](#) qui : Cette politique inclut les autorisations permettant d'exécuter des commandes SQL pour copier, charger, télécharger, interroger et analyser des données sur Amazon Redshift. Cette politique accorde également les autorisations nécessaires pour exécuter les instructions sélectionnées pour les services associés, tels qu'Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon Amazon ou AWS Glue.

Utilisation de cette politique de politique utilisée

Vous pouvez AmazonRedshiftAllCommandsFullAccess les associer à vos utilisateurs, groupes et rôles.

Les politiques détaillées des politiques

- Type : politique AWS gérée
- Heure de création : 4 novembre 2021, 00:48 UTC
- Heure modifiée : 25 novembre 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON de politique

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées gérées et évoluez vers les autorisations de moindre privilège gérées et évoluez vers les autorisations de moindre privilège gérées](#)

AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess est une [politiqueAWS gérée](#) qui : Cette politique fournit un accès complet aux fonctions de données Amazon Redshift. Cette politique permet également d'accéder de manière limitée à d'autres services requis.

Utilisation de cette politique

Vous pouvez les associer AmazonRedshiftDataFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 septembre 2020, 19:23 UTC
- Heure modifiée : 7 avril 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "Sid" : "DataAPIPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift-data:BatchExecuteStatement",
      "redshift-data:ExecuteStatement",
      "redshift-data:CancelStatement",
      "redshift-data:ListStatements",
      "redshift-data:GetStatementResult",
      "redshift-data:DescribeStatement",
      "redshift-data:ListDatabases",
      "redshift-data:ListSchemas",
      "redshift-data:ListTables",
      "redshift-data:DescribeTable"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
      }
    }
  },
  {
    "Sid" : "GetCredentialsForAPIUser",
    "Effect" : "Allow",
    "Action" : "redshift:GetClusterCredentials",
    "Resource" : [
      "arn:aws:redshift:*:*:dbname:*/*",
      "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
    ]
  },
  {
    "Sid" : "GetCredentialsWithFederatedIAMCredentials",
    "Effect" : "Allow",
    "Action" : "redshift:GetClusterCredentialsWithIAM",
    "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
  },

```

```

{
  "Sid" : "GetCredentialsForServerless",
  "Effect" : "Allow",
  "Action" : "redshift-serverless:GetCredentials",
  "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/RedshiftDataFullAccess" : "*"
    }
  }
},
{
  "Sid" : "DenyCreateAPIUser",
  "Effect" : "Deny",
  "Action" : "redshift:CreateClusterUser",
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
  ]
},
{
  "Sid" : "ServiceLinkedRole",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "redshift-data.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRedshiftFullAccess

AmazonRedshiftFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Redshift via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonRedshiftFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 07 juillet 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
```



```

    "sns:CreateTopic",
    "sns:Get*",
    "sns:List*",
    "cloudwatch:Describe*",
    "cloudwatch:Get*",
    "cloudwatch:List*",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:EnableAlarmActions",
    "cloudwatch:DisableAlarmActions",
    "tag:GetResources",
    "tag:UntagResources",
    "tag:GetTagValues",
    "tag:GetTagKeys",
    "tag:TagResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "redshift.amazonaws.com"
    }
  }
},
{
  "Sid" : "DataAPIPermissions",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:ListStatements",
    "redshift-data:GetStatementResult",
    "redshift-data:DescribeStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}

```

```
  },
  {
    "Sid" : "SecretsManagerListPermissions",
    "Action" : [
      "secretsmanager:ListSecrets"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerCreateGetPermissions",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:TagResource"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRedshiftQueryEditor

AmazonRedshiftQueryEditor est une [politique AWS gérée](#) qui : fournit un accès complet à l'éditeur de requêtes Amazon Redshift et aux requêtes enregistrées via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonRedshiftQueryEditor` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 4 octobre 2018, 22:50 UTC
- Heure modifiée : 16 février 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",

```

```

    "redshift:CreateSavedQuery",
    "redshift>DeleteSavedQueries",
    "redshift:ModifySavedQuery"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DataAPIPermissions",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "DataAPIIAMSessionPermissionsRestriction",
  "Action" : [
    "redshift-data:GetStatementResult",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:ListStatements"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "SecretsManagerListPermissions",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerCreateGetPermissions",

```

```
"Action" : [
  "secretsmanager:CreateSecret",
  "secretsmanager:GetSecretValue",
  "secretsmanager:TagResource"
],
"Effect" : "Allow",
"Resource" : "arn:aws:secretsmanager:*:*:secret:*",
"Condition" : {
  "StringEquals" : {
    "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRedshiftQueryEditorV2FullAccess

AmazonRedshiftQueryEditorV2FullAccess est une [politique AWS gérée](#) qui : accorde un accès complet aux opérations et aux ressources d'Amazon Redshift Query Editor V2. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations permettant de répertorier les clusters Amazon Redshift, de lire les clés et les alias dans AWS KMS et de gérer les secrets de Query Editor V2 dans Secrets Manager AWS .

Utilisation de cette politique

Vous pouvez vous associer AmazonRedshiftQueryEditorV2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 24 septembre 2021, 14:06 UTC
- Heure modifiée : 21 février 2024, 17:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
    "secretsmanager:GetSecretValue",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
},
{
  "Sid" : "ResourceGroupsTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:*",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftQueryEditorV2NoSharing

AmazonRedshiftQueryEditorV2NoSharing est une [politique AWS gérée](#) qui : permet de travailler avec Amazon Redshift Query Editor V2 sans partager de ressources. Le principal autorisé peut uniquement lire, mettre à jour et supprimer ses propres ressources, mais ne peut pas les

partager. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations permettant de répertorier les clusters Amazon Redshift et de gérer les secrets de l'éditeur de requête V2 du principal dans AWS Secrets Manager.

Utilisation de cette politique

Vous pouvez vous associer `AmazonRedshiftQueryEditorV2NoSharing` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:18 UTC
- Heure modifiée : 21 février 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
```



```

    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager>DeleteSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "ResourceGroupsTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",

```

```

    "sqlworkbench:ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench:ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench:ListTaggedResources",
    "sqlworkbench:ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench:ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:user}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench>DeleteChart",
    "sqlworkbench>DeleteConnection",
    "sqlworkbench>DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",

```

```

    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench>DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench>CreateNotebookCell",
    "sqlworkbench>DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench>CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-resource-owner"
    },
    "StringEquals" : {

```

```
        "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
        "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftQueryEditorV2ReadSharing

AmazonRedshiftQueryEditorV2ReadSharing est une [politique AWS gérée](#) qui : permet de travailler avec Amazon Redshift Query Editor V2 avec un partage limité des ressources. Le mandant autorisé peut lire, écrire et partager ses propres ressources. Le principal autorisé peut lire les ressources partagées avec son équipe mais ne peut pas les mettre à jour. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations permettant de répertorier les clusters Amazon Redshift et de gérer les secrets de l'éditeur de requête V2 du principal dans AWS Secrets Manager.

Utilisation de cette politique

Vous pouvez vous associer AmazonRedshiftQueryEditorV2ReadSharing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:22 UTC
- Heure modifiée : 21 février 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateFolder",
    "sqlworkbench:PutTab",
    "sqlworkbench:BatchDeleteFolder",
    "sqlworkbench>DeleteTab",
    "sqlworkbench:GenerateSession",
    "sqlworkbench:GetAccountInfo",
    "sqlworkbench:GetAccountSettings",
    "sqlworkbench:GetUserInfo",
    "sqlworkbench:GetUserWorkspaceSettings",
    "sqlworkbench:PutUserWorkspaceSettings",
    "sqlworkbench>ListConnections",
    "sqlworkbench>ListFiles",
    "sqlworkbench>ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench>ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench>ListTaggedResources",
    "sqlworkbench>ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench>ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench>CreateConnection",
```

```

    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:user}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:DeleteChart",
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench:DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookCell",
    "sqlworkbench:DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
  ]
}

```

```

    "sqlworkbench:CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-resource-owner"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

AmazonRedshiftQueryEditorV2ReadWriteSharing est une [politique AWS gérée](#) qui : permet de travailler avec Amazon Redshift Query Editor V2 avec partage de ressources. Le mandant autorisé peut lire, écrire et partager ses propres ressources. Le principal autorisé peut lire et mettre à jour les ressources partagées avec son équipe. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations permettant de répertorier les clusters Amazon Redshift et de gérer les secrets de l'éditeur de requête V2 du principal dans AWS Secrets Manager.

Utilisation de cette politique

Vous pouvez vous associer AmazonRedshiftQueryEditorV2ReadWriteSharing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:25 UTC
- Heure modifiée : 21 février 2024, 17h30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    }
  ]
}
```

```
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",
      "sqlworkbench>ListTabs",
      "sqlworkbench:UpdateFolder",
      "sqlworkbench>ListRedshiftClusters",
      "sqlworkbench:DriverExecute",
      "sqlworkbench>ListTaggedResources",
      "sqlworkbench>ListQueryExecutionHistory",
      "sqlworkbench:GetQueryExecutionHistory",
      "sqlworkbench>ListNotebooks",
      "sqlworkbench:GetSchemaInference",
      "sqlworkbench:GetAutocompletionMetadata",
      "sqlworkbench:GetAutocompletionResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateConnection",
      "sqlworkbench:CreateSavedQuery",
      "sqlworkbench:CreateChart",
      "sqlworkbench:CreateNotebook",
      "sqlworkbench:DuplicateNotebook",
      "sqlworkbench:CreateNotebookFromVersion",
      "sqlworkbench:ImportNotebook"
    ],
    "Resource" : "*",
```

```
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:user}"
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:DeleteChart",
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench>DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench>CreateNotebookCell",
    "sqlworkbench>DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench>CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
}
```

```

    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:TagResource",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "sqlworkbench-resource-owner"
      },
      "StringEquals" : {
        "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
        "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:GetChart",
      "sqlworkbench:GetConnection",
      "sqlworkbench:GetSavedQuery",
      "sqlworkbench:ListSavedQueryVersions",
      "sqlworkbench:ListTagsForResource",
      "sqlworkbench:UpdateChart",
      "sqlworkbench:UpdateConnection",
      "sqlworkbench:UpdateSavedQuery",
      "sqlworkbench:AssociateConnectionWithTab",
      "sqlworkbench:AssociateQueryWithTab",
      "sqlworkbench:AssociateConnectionWithChart",
      "sqlworkbench:AssociateNotebookWithTab",
      "sqlworkbench:GetNotebook",
      "sqlworkbench:DuplicateNotebook",
      "sqlworkbench:BatchGetNotebookCell",
      "sqlworkbench:ListNotebookVersions",
      "sqlworkbench:GetNotebookVersion",
      "sqlworkbench>CreateNotebookFromVersion",

```

```

    "sqlworkbench:ExportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:UntagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftReadOnlyAccess

AmazonRedshiftReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Redshift via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonRedshiftReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 8 février 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



```
"Sid" : "AmazonRedshiftReadOnlyAccess",
"Action" : [
  "redshift:Describe*",
  "redshift:ListRecommendations",
  "redshift:ViewQueriesInConsole",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAddresses",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcs",
  "ec2:DescribeInternetGateways",
  "sns:Get*",
  "sns:List*",
  "cloudwatch:Describe*",
  "cloudwatch:List*",
  "cloudwatch:Get*"
],
"Effect" : "Allow",
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRedshiftServiceLinkedRolePolicy

AmazonRedshiftServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : autorise Amazon Redshift à appeler des AWS services en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 18 septembre 2017, 19:19 UTC
- Heure modifiée : 15 mars 2024, 20h00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    }
  ],
  {
    "Sid" : "PublicAccessReleaseEip",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ReleaseAddress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/Redshift" : "true"
      }
    }
  }
],
{
  "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/redshift/*"
  ]
},
{
  "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
```

```

    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
    ]
  },
  {
    "Sid" : "CreateSecurityGroupWithTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/Redshift" : "true"
      }
    }
  },
  {
    "Sid" : "SecurityGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:ModifySecurityGroupRules",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/Redshift" : "true"
      }
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "CreateSecurityGroup",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Sid" : "CreateTagsOnResources",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:internet-gateway/*",
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateVpc",
          "CreateSecurityGroup",
          "CreateSubnet",
          "CreateInternetGateway",
          "CreateRouteTable",
          "AllocateAddress"
        ]
      }
    }
  },
  {
    "Sid" : "VPCPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeInternetGateways",
```

```

    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Redshift-Serverless",
        "AWS/Redshift"
      ]
    }
  }
},
{
  "Sid" : "SecretManager",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:UpdateSecret",
    "secretsmanager:UpdateSecretVersionStage",
    "secretsmanager:RotateSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:redshift!*"
  ],
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},

```

```
{
  "Sid" : "SecretsManagerRandomPassword",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IPV6Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ]
},
{
  "Sid" : "ServiceQuotasToCheckCustomerLimits",
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ],
  "Resource" : [
    "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
    "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRekognitionCustomLabelsFullAccess

AmazonRekognitionCustomLabelsFullAccess est une [politique AWS gérée](#) qui : Cette politique spécifie les autorisations de reconnaissance et s3 requises par la fonctionnalité Amazon Rekognition Custom Labels.

Utilisation de cette stratégie

Vous pouvez AmazonRekognitionCustomLabelsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 janvier 2020, 19:18 UTC
- Heure modifiée : 16 août 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
```



```

    "s3:GetObjectAcl",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : "arn:aws:s3:::*custom-labels*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rekognition:CreateProject",
    "rekognition:CreateProjectVersion",
    "rekognition:StartProjectVersion",
    "rekognition:StopProjectVersion",
    "rekognition:DescribeProjects",
    "rekognition:DescribeProjectVersions",
    "rekognition:DetectCustomLabels",
    "rekognition>DeleteProject",
    "rekognition>DeleteProjectVersion",
    "rekognition:TagResource",
    "rekognition:UntagResource",
    "rekognition:ListTagsForResource",
    "rekognition:CreateDataset",
    "rekognition:ListDatasetEntries",
    "rekognition:ListDatasetLabels",
    "rekognition:DescribeDataset",
    "rekognition:UpdateDatasetEntries",
    "rekognition:DistributeDatasetEntries",
    "rekognition>DeleteDataset",
    "rekognition:CopyProjectVersion",
    "rekognition:PutProjectPolicy",
    "rekognition:ListProjectPolicies",
    "rekognition>DeleteProjectPolicy"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRekognitionFullAccess

AmazonRekognitionFullAccess est une [politiqueAWS gérée](#) qui : Accès à toutes les API Amazon Rekognition

Utilisation de cette stratégie

Vous pouvez AmazonRekognitionFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 novembre 2016, 14:40 UTC
- Heure modifiée : 30 novembre 2016, 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRekognitionReadOnlyAccess

AmazonRekognitionReadOnlyAccess est une [politique AWS gérée](#) qui : Accès à toutes les API de reconnaissance Read

Utilisation de cette politique

Vous pouvez vous associer AmazonRekognitionReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 14:58 UTC
- Heure modifiée : 8 novembre 2023, 18h30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRekognitionServiceRole

AmazonRekognitionServiceRole est une [politique AWS gérée](#) qui : Permet à Rekognition d'appeler AWS des services en votre nom.

Utilisation de cette stratégie

Vous pouvez les associer AmazonRekognitionServiceRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 29 novembre 2017, 16:52 UTC
- Heure modifiée : 29 novembre 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53AutoNamingFullAccess

AmazonRoute53AutoNamingFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à toutes les actions de dénomination automatique Route 53.

Utilisation de cette stratégie

Vous pouvez AmazonRoute53AutoNamingFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 janvier 2018, 18:40 UTC
- Heure modifiée : 18 janvier 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
```

```
    "route53:CreateHealthCheck",
    "route53:GetHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:UpdateHealthCheck",
    "ec2:DescribeVpcs",
    "ec2:DescribeRegions",
    "servicediscovery:*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53AutoNamingReadOnlyAccess

AmazonRoute53AutoNamingReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à toutes les actions de dénomination automatique Route 53.

Utilisation de cette stratégie

Vous pouvez AmazonRoute53AutoNamingReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 janvier 2018, 03:02 UTC
- Heure modifiée : 18 janvier 2018, 03:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess est une [politique AWS gérée](#) qui : fournit un accès au niveau du déclarant aux actions de dénomination automatique Route 53.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonRoute53AutoNamingRegistrantAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 12 mars 2018, 22:33 UTC
- Heure modifiée : 12 mars 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53DomainsFullAccess

AmazonRoute53DomainsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les actions de Route53 Domains et Create Hosted Zone pour permettre la création de zones hébergées dans le cadre des enregistrements de domaines.

Utilisation de cette stratégie

Vous pouvez AmazonRoute53DomainsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53DomainsReadOnlyAccess

AmazonRoute53DomainsReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès à la liste et aux actions des domaines Route53.

Utilisation de cette stratégie

Vous pouvez AmazonRoute53DomainsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53FullAccess

AmazonRoute53FullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à tous les Amazon Route 53 via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonRoute53FullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 20 décembre 2018, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
```

```

    "cloudfront:ListDistributions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticbeanstalk:DescribeEnvironments",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRegions",
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : "arn:aws:apigateway:*::/domainnames"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53ReadOnlyAccess

AmazonRoute53ReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à tous les Amazon Route 53 via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonRoute53ReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 15 novembre 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53RecoveryClusterFullAccess

AmazonRoute53RecoveryClusterFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet au cluster de restauration Amazon Route 53

Utilisation de cette stratégie

Vous pouvez AmazonRoute53RecoveryClusterFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 18:37 UTC
- Heure modifiée : 18 août 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ]
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

AmazonRoute53RecoveryClusterReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule au cluster de restauration Amazon Route 53

Utilisation de cette stratégie

Vous pouvez AmazonRoute53RecoveryClusterReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 août 2021, 17:36 UTC
- Heure modifiée : 1 avril 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53RecoveryControlConfigFullAccess

AmazonRoute53RecoveryControlConfigFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Route 53 Recovery Control Config

Utilisation de cette stratégie

Vous pouvez AmazonRoute53RecoveryControlConfigFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 août 2021, 17:48 UTC

- Heure modifiée : 18 août 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Route 53 Recovery Control Config

Utilisation de cette politique

Vous pouvez vous associer `AmazonRoute53RecoveryControlConfigReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 18:01 UTC
- Heure modifiée : 18 octobre 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",

```

```
    "route53-recovery-control-config:ListRoutingControls",
    "route53-recovery-control-config:ListSafetyRules",
    "route53-recovery-control-config:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonRoute53RecoveryReadinessFullAccess

AmazonRoute53RecoveryReadinessFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon Route 53 Recovery Readiness

Utilisation de cette stratégie

Vous pouvez AmazonRoute53RecoveryReadinessFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 16:45 UTC
- Heure modifiée : 18 août 2021, 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

AmazonRoute53RecoveryReadinessReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Route 53 Recovery Readiness

Utilisation de cette stratégie

Vous pouvez AmazonRoute53RecoveryReadinessReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 18 août 2021, 18:11 UTC
- Heure modifiée : 09 novembre 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
```



```
    "route53-recovery-readiness:GetCellReadinessSummary"
  ],
  "Resource" : "arn:aws:route53-recovery-readiness::*:*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53ResolverFullAccess

AmazonRoute53ResolverFullAccess est une [politique AWS gérée](#) qui : Politique d'accès complet au résolveur Route 53

Utilisation de cette stratégie

Vous pouvez les associer AmazonRoute53ResolverFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 mai 2019, 18:10 UTC
- Heure modifiée : 17 juillet 2020, 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess est une [politique AWS gérée](#) qui : Politique en lecture seule pour Route 53 Resolver

Utilisation de cette stratégie

Vous pouvez les associer AmazonRoute53ResolverReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 mai 2019, 18:11 UTC
- Heure modifiée : 27 septembre 2019, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ]
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonS3FullAccess

AmazonS3FullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à tous les compartiments via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonS3FullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 27 septembre 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy est une [politique AWS gérée](#) qui : fournit des autorisations aux fonctions AWS Lambda pour interagir avec Amazon S3 Object Lambda. Autorise également Lambda à écrire dans CloudWatch Logs.

Utilisation de cette stratégie

Vous pouvez AmazonS3ObjectLambdaExecutionRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 18 août 2021, 10:07 UTC

- Heure modifiée : 18 août 2021, 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonS3OutpostsFullAccess

AmazonS3OutpostsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon S3 sur Outposts via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer AmazonS3OutpostsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 octobre 2020, 17:26 UTC
- Heure modifiée : 2 octobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonS3OutpostsReadOnlyAccess

AmazonS3OutpostsReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon S3 sur Outposts via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez `AmazonS3OutpostsReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 2 octobre 2020, 18:55 UTC
- Heure modifiée : 2 octobre 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
```

```
    "datasync:DescribeLocation*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeNetworkInterfaces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "outposts:ListOutposts",
    "outposts:GetOutpost"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonS3ReadOnlyAccess

AmazonS3ReadOnlyAccess est un [AWS politique gérée](#) qui : fournit un accès en lecture seule à tous les compartiments via le AWS Management Console.

Utilisation de cette politique

Vous pouvez joindre AmazonS3ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 06 février 2015, 18:40 UTC
- Heure modifiée :10 août 2023, 21h31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

Version de la politique

Version de la politique : v3(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations du moindre privilège](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicyest une [politiqueAWS gérée qui : Politique](#) de rôle de service utilisée par le serviceService AWS Catalog pour approvisionner des produits du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes CodePipeline CodeBuild CodeCommit, notamment, CloudFormation, Glue, etc.

Utilisation de cette stratégie

Vous pouvezAmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2020, 18:48 UTC
- Heure modifiée : 2 août 2022, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:PATCH",
      "apigateway:DELETE"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/sagemaker:launch-source" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:POST"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "sagemaker:launch-source"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:PATCH"
    ],
    "Resource" : [
      "arn:aws:apigateway:*::/account"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
```

```

    "cloudformation:UpdateStack",
    "cloudformation>DeleteStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
  "Condition" : {
    "ArnLikeIfExists" : {
      "cloudformation:RoleArn" : [
        "arn:aws:sts:*:*:assumed-role/AmazonSageMakerServiceCatalog*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "cloudformation:ValidateTemplate"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:UpdateProject"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codecommit:CreateCommit",
    "codecommit:CreateRepository",

```

```

        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
    ],
    "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "codecommit:ListRepositories"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline>DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
    ],
    "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringLike" : {
            "aws:TagKeys" : [
                "sagemaker:launch-source"
            ]
        }
    }
}

```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cognito-idp:CreateGroup",
      "cognito-idp:CreateUserPoolDomain",
      "cognito-idp:CreateUserPoolClient",
      "cognito-idp>DeleteGroup",
      "cognito-idp>DeleteUserPool",
      "cognito-idp>DeleteUserPoolClient",
      "cognito-idp>DeleteUserPoolDomain",
      "cognito-idp:DescribeUserPool",
      "cognito-idp:DescribeUserPoolClient",
      "cognito-idp:UpdateUserPool",
      "cognito-idp:UpdateUserPoolClient"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/sagemaker:launch-source" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr>DeleteRepository",
      "ecr:TagResource"
    ],
    "Resource" : [
      "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events>DeleteRule",
      "events:DisableRule",
      "events:EnableRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ]
  }
}
```



```

    ],
    "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose>DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateDatabase",
        "glue>DeleteDatabase"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateClassifier",
        "glue>DeleteClassifier",
        "glue>DeleteCrawler",
        "glue>DeleteJob",
        "glue>DeleteTrigger",
        "glue>DeleteWorkflow",
        "glue:StopCrawler"
    ],
    "Resource" : [
        "*"
    ]
}

```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateWorkflow"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:workflow/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateJob"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:job/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateCrawler",
      "glue:GetCrawler"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:crawler/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateTrigger",
      "glue:GetTrigger"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:trigger/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
  },
```

```

    "Resource" : [
      "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration",
      "lambda:InvokeFunction",
      "lambda:RemovePermission"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "lambda:TagResource",
    "Resource" : [
      "arn:aws:lambda:*:*:function:sagemaker-*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : [
          "sagemaker:*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs>DeleteLogGroup",
      "logs>DeleteLogStream",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:PutRetentionPolicy"
    ],
  },

```

```

    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
      "arn:aws:logs:*:*:log-group::log-stream:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : [
      "arn:aws:s3:::sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3>DeleteBucket",
      "s3>DeleteBucketPolicy",
      "s3:GetBucketPolicy",
      "s3:PutBucketAcl",
      "s3:PutBucketNotification",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketLogging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketCORS",
      "s3:PutBucketTagging",
      "s3:PutObjectTagging"
    ],
    "Resource" : "arn:aws:s3:::sagemaker-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [

```

```

    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateModel",
    "sagemaker:CreateWorkteam",
    "sagemaker>DeleteEndpoint",
    "sagemaker>DeleteEndpointConfig",
    "sagemaker>DeleteModel",
    "sagemaker>DeleteWorkteam",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeWorkteam",
    "sagemaker:CreateCodeRepository",
    "sagemaker:DescribeCodeRepository",
    "sagemaker:UpdateCodeRepository",
    "sagemaker>DeleteCodeRepository"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:endpoint/*",
    "arn:aws:sagemaker:*:*:endpoint-config/*",
    "arn:aws:sagemaker:*:*:model/*",
    "arn:aws:sagemaker:*:*:pipeline/*",
    "arn:aws:sagemaker:*:*:project/*",
    "arn:aws:sagemaker:*:*:model-package*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : [
        "sagemaker:*"
      ]
    }
  }
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "sagemaker:CreateImage",
  "sagemaker>DeleteImage",
  "sagemaker:DescribeImage",
  "sagemaker:UpdateImage",
  "sagemaker>ListTags"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:image/*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states>CreateStateMachine",
    "states>DeleteStateMachine",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
  "Condition" : {
    "StringEquals" : {
      "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerCanvasAIServicesAccess

AmazonSageMakerCanvasAIServicesAccess est une [politique AWS gérée](#) qui : autorise Amazon SageMaker Canvas à utiliser des services d'IA pour prendre en charge des solutions d'IA prêtes à l'emploi. Cette politique ajoutera d'autres autorisations mutantes pour les services à mesure qu'Amazon SageMaker Canvas ajoutera du support.

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerCanvasAIServicesAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2023, 22:36 UTC
- Heure modifiée : 29 novembre 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
```

```

    "extract:StartDocumentAnalysis",
    "extract:StartExpenseAnalysis",
    "extract:GetDocumentAnalysis",
    "extract: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"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccess est une [politique AWS gérée](#) qui : Cette politique accorde les autorisations d'utiliser Amazon Bedrock dans SageMaker Canvas en fournissant un accès à des services en aval tels que S3.

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerCanvasBedrockAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 février 2024, 18:37 UTC
- Heure modifiée : 2 février 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:s3:::sagemaker-*/Canvas",
      "arn:aws:s3:::sagemaker-*/Canvas/*"
    ]
  },
  {
    "Sid" : "S3BucketAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::sagemaker-*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerCanvasDataPrepFullAccess

AmazonSageMakerCanvasDataPrepFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux SageMaker ressources et aux opérations Amazon pour la préparation des données dans Canvas. La politique fournit également un accès sélectif aux services connexes (par exemple, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue EventBridge, Secrets Manager). Cette politique doit être associée au rôle d'exécution Amazon SageMaker Domain/User Profile.

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerCanvasDataPrepFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 octobre 2023, 22:56 UTC
- Heure modifiée : 8 décembre 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
```

```

    "sagemaker:DescribeProcessingJob",
    "sagemaker:AddTags"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
},
{
  "Sid" : "SageMakerProcessingJobListOperation",
  "Effect" : "Allow",
  "Action" : "sagemaker:ListProcessingJobs",
  "Resource" : "*"
},
{
  "Sid" : "SageMakerPipelineOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribePipeline",
    "sagemaker:CreatePipeline",
    "sagemaker:UpdatePipeline",
    "sagemaker>DeletePipeline",
    "sagemaker:StartPipelineExecution",
    "sagemaker>ListPipelineExecutionSteps",
    "sagemaker:DescribePipelineExecution"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
},
{
  "Sid" : "KMSListOperations",
  "Effect" : "Allow",
  "Action" : "kms:ListAliases",
  "Resource" : "*"
},
{
  "Sid" : "KMSOperations",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Sid" : "S3Operations",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3>DeleteObject",

```

```

    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:AbortMultipartUpload"
  ],
  "Resource" : [
    "arn:aws:s3:::*SageMaker*",
    "arn:aws:s3:::*Sagemaker*",
    "arn:aws:s3:::*sagemaker*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "S3GetObjectOperation",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/SageMaker" : "true"
    },
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "S3ListOperations",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMListOperations",
  "Effect" : "Allow",
  "Action" : "iam:ListRoles",
  "Resource" : "*"
},

```

```
{
  "Sid" : "IAMGetOperations",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "IAMPassOperation",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com",
        "events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "EventBridgePutOperation",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events::*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:PutTargets"
  ],
  "Resource" : "arn:aws:events::*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
}
```



```

    }
  }
},
{
  "Sid" : "EventBridgeTagBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:TagResource"
  ],
  "Resource" : "arn:aws:events:*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeListTagOperation",
  "Effect" : "Allow",
  "Action" : "events:ListTagsForResource",
  "Resource" : "*"
},
{
  "Sid" : "GlueOperations",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:SearchTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "EMROperations",
  "Effect" : "Allow",
  "Action" : [
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups"
  ]
}

```

```
    ],
    "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
  },
  {
    "Sid" : "EMRListOperation",
    "Effect" : "Allow",
    "Action" : "elasticmapreduce:ListClusters",
    "Resource" : "*"
  },
  {
    "Sid" : "AthenaListDataCatalogOperation",
    "Effect" : "Allow",
    "Action" : "athena:ListDataCatalogs",
    "Resource" : "*"
  },
  {
    "Sid" : "AthenaQueryExecutionOperations",
    "Effect" : "Allow",
    "Action" : [
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:StartQueryExecution",
      "athena:StopQueryExecution"
    ],
    "Resource" : "arn:aws:athena:*:*:workgroup/*"
  },
  {
    "Sid" : "AthenaDataCatalogOperations",
    "Effect" : "Allow",
    "Action" : [
      "athena:ListDatabases",
      "athena:ListTableMetadata"
    ],
    "Resource" : "arn:aws:athena:*:*:datacatalog/*"
  },
  {
    "Sid" : "RedshiftOperations",
    "Effect" : "Allow",
    "Action" : [
      "redshift-data:DescribeStatement",
      "redshift-data:CancelStatement",
      "redshift-data:GetStatementResult"
    ],
    "Resource" : "*"
  }
```

```

},
{
  "Sid" : "RedshiftArnBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ],
  "Resource" : "arn:aws:redshift:*:*:cluster:*"
},
{
  "Sid" : "RedshiftGetCredentialsOperation",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentials",
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "SecretsManagerARNBasedOperation",
  "Effect" : "Allow",
  "Action" : "secretsmanager:CreateSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
},
{
  "Sid" : "SecretManagerTagBasedOperation",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",

```

```
    "Action" : "rds:DescribeDBInstances",
    "Resource" : "*"
  },
  {
    "Sid" : "LoggingOperation",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccess est une [politique AWS gérée](#) qui : permet à Amazon SageMaker Canvas de créer, de gérer et d'afficher les détails des points de terminaison créés via Canvas. Permet à Amazon SageMaker Canvas de récupérer les métriques d'invocation des terminaux à partir de CloudWatch.

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerCanvasDirectDeployAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 06 octobre 2023, 18:11 UTC

- Heure modifiée : 6 octobre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker>DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccess est une [stratégie AWS gérée](#) qui : Cette politique accorde les autorisations généralement requises pour utiliser SageMaker Canvas avec Amazon Forecast.

Utilisation de cette politique

Vous pouvez AmazonSageMakerCanvasForecastAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 24 août 2022, 20:04 UTC
- Heure modifiée : 24 août 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerCanvasFullAccess

AmazonSageMakerCanvasFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux ressources et aux opérations d'Amazon SageMaker Canvas. La politique fournit également

un accès sélectif aux services connexes (par exemple, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager et Forecast). Cette politique doit être associée au rôle d'exécution Amazon SageMaker Domain/User Profile.

Utilisation de cette politique

Vous pouvez vous associer `AmazonSageMakerCanvasFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 septembre 2022, 00:44 UTC
- Heure modifiée : 24 janvier 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ]
    }
  ],
}
```



```

    "Resource" : "*"
  },
  {
    "Sid" : "SageMakerPackageGroupOperations",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateModelPackageGroup",
      "sagemaker:CreateModelPackage",
      "sagemaker:DescribeModelPackageGroup",
      "sagemaker:DescribeModelPackage"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:model-package/*",
      "arn:aws:sagemaker:*:*:model-package-group/*"
    ]
  },
  {
    "Sid" : "SageMakerTrainingOperations",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateCompilationJob",
      "sagemaker:CreateEndpoint",
      "sagemaker:CreateEndpointConfig",
      "sagemaker:CreateModel",
      "sagemaker:CreateProcessingJob",
      "sagemaker:CreateAutoMLJob",
      "sagemaker:CreateAutoMLJobV2",
      "sagemaker>DeleteEndpoint",
      "sagemaker:DescribeCompilationJob",
      "sagemaker:DescribeEndpoint",
      "sagemaker:DescribeEndpointConfig",
      "sagemaker:DescribeModel",
      "sagemaker:DescribeProcessingJob",
      "sagemaker:DescribeAutoMLJob",
      "sagemaker:DescribeAutoMLJobV2",
      "sagemaker:ListCandidatesForAutoMLJob",
      "sagemaker:AddTags",
      "sagemaker>DeleteApp"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:*Canvas*",
      "arn:aws:sagemaker:*:*:*canvas*",
      "arn:aws:sagemaker:*:*:*model-compilation-*"
    ]
  }
]

```

```
},
{
  "Sid" : "SageMakerHostingOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DeleteEndpointConfig",
    "sagemaker:DeleteModel",
    "sagemaker:InvokeEndpoint",
    "sagemaker:UpdateEndpointWeightsAndCapacities",
    "sagemaker:InvokeEndpointAsync"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:*Canvas*",
    "arn:aws:sagemaker:*:*:*canvas*"
  ]
},
{
  "Sid" : "EC2VPCOperation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ECROperations",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetAuthorizationToken"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMGetOperations",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
```

```
    ],
    "Resource" : "arn:aws:iam::*:role/*"
  },
  {
    "Sid" : "IAMPassOperation",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  }
},
{
  "Sid" : "LoggingOperation",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
},
{
  "Sid" : "S3Operations",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:CreateBucket",
    "s3:GetBucketCors",
    "s3:GetBucketLocation"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ]
}
}
```

```

    "Sid" : "ReadSageMakerJumpstartArtifacts",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : [
      "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
      "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
      "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
      "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
      "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
    ]
  },
  {
    "Sid" : "S3ListOperations",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GlueOperations",
    "Effect" : "Allow",
    "Action" : "glue:SearchTables",
    "Resource" : [
      "arn:aws:glue:*:*:table/*/*",
      "arn:aws:glue:*:*:database/*",
      "arn:aws:glue:*:*:catalog"
    ]
  },
  {
    "Sid" : "SecretsManagerARNBasedOperation",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DescribeSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:CreateSecret",
      "secretsmanager:PutResourcePolicy"
    ]
  },

```

```

    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    ]
  },
  {
    "Sid" : "SecretManagerTagBasedOperation",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DescribeSecret",
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/SageMaker" : "true"
      }
    }
  },
  {
    "Sid" : "RedshiftOperations",
    "Effect" : "Allow",
    "Action" : [
      "redshift-data:ExecuteStatement",
      "redshift-data:DescribeStatement",
      "redshift-data:CancelStatement",
      "redshift-data:GetStatementResult",
      "redshift-data:ListSchemas",
      "redshift-data:ListTables",
      "redshift-data:DescribeTable"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RedshiftGetCredentialsOperation",
    "Effect" : "Allow",
    "Action" : [
      "redshift:GetClusterCredentials"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
      "arn:aws:redshift:*:*:dbname:*"
    ]
  },
  {

```

```
"Sid" : "ForecastOperations",
"Effect" : "Allow",
"Action" : [
  "forecast:CreateExplainabilityExport",
  "forecast:CreateExplainability",
  "forecast:CreateForecastEndpoint",
  "forecast:CreateAutoPredictor",
  "forecast:CreateDatasetImportJob",
  "forecast:CreateDatasetGroup",
  "forecast:CreateDataset",
  "forecast:CreateForecast",
  "forecast:CreateForecastExportJob",
  "forecast:CreatePredictorBacktestExportJob",
  "forecast:CreatePredictor",
  "forecast:DescribeExplainabilityExport",
  "forecast:DescribeExplainability",
  "forecast:DescribeAutoPredictor",
  "forecast:DescribeForecastEndpoint",
  "forecast:DescribeDatasetImportJob",
  "forecast:DescribeDataset",
  "forecast:DescribeForecast",
  "forecast:DescribeForecastExportJob",
  "forecast:DescribePredictorBacktestExportJob",
  "forecast:GetAccuracyMetrics",
  "forecast:InvokeForecastEndpoint",
  "forecast:GetRecentForecastContext",
  "forecast:DescribePredictor",
  "forecast:TagResource",
  "forecast>DeleteResourceTree"
],
"Resource" : [
  "arn:aws:forecast:*:*:*Canvas*"
]
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",
  "Action" : "rds:DescribeDBInstances",
  "Resource" : "*"
},
{
  "Sid" : "IAMPassOperationForForecast",
  "Effect" : "Allow",
  "Action" : [
```

```

    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "forecast.amazonaws.com"
    }
  }
},
{
  "Sid" : "AutoscalingOperations",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:RegisterScalableTarget"
  ],
  "Resource" : "arn:aws:application-autoscaling::*:scalable-target/*",
  "Condition" : {
    "StringEquals" : {
      "application-autoscaling:service-namespace" : "sagemaker",
      "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
    }
  }
},
{
  "Sid" : "AsyncEndpointOperations",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "sagemaker:DescribeEndpointConfig"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SageMakerCloudWatchUpdate",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch::*:alarm:TargetTracking*"
  ],

```

```
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerClusterInstanceRolePolicy

AmazonSageMakerClusterInstanceRolePolicy est une [politique AWS gérée](#) qui : Cette politique accorde les autorisations généralement nécessaires pour utiliser Amazon SageMaker Cluster.

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerClusterInstanceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 15:11 UTC
- Heure modifiée : 29 novembre 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    }
  ]
}
```

```
]
},
{
  "Sid" : "CloudwatchPutMetricDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
    }
  }
},
{
  "Sid" : "DataRetrievalFromS3BucketPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::sagemaker-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "SSMConnectivityPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy est une [stratégie AWS gérée](#) qui : Stratégie gérée pour le rôle lié à un service pour Amazon SageMaker Core Services

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 décembre 2020, 21:40 UTC
- Heure modifiée : 21 décembre 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy est une [politiqueAWS gérée](#) qui : fournit les autorisations nécessaires à SageMaker Edge pour créer et gérer un parc d'appareils pour le client à l'aide de la connexion cloud par défaut.

Utilisation de cette stratégie

Vous pouvez AmazonSageMakerEdgeDeviceFleetPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 8 décembre 2020, 16:17 UTC
- Heure modifiée : 8 décembre 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Sid" : "DeviceS3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:GetBucketLocation"
    ],
    "Resource" : [
      "arn:aws:s3:::*SageMaker*",
      "arn:aws:s3:::*Sagemaker*",
      "arn:aws:s3:::*sagemaker*"
    ]
  },
  {
    "Sid" : "SageMakerEdgeApis",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:SendHeartbeat",
      "sagemaker:GetDeviceRegistration"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateIoTRoleAlias",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateRoleAlias",
      "iot:DescribeRoleAlias",
      "iot:UpdateRoleAlias",
      "iot:ListTagsForResource",
      "iot:TagResource"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
    ]
  },
  {
    "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
```

```

    "arn:aws:iam::*:role/*SageMaker*",
    "arn:aws:iam::*:role/*Sagemaker*",
    "arn:aws:iam::*:role/*sagemaker*"
  ]
},
{
  "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/*SageMaker*",
    "arn:aws:iam::*:role/*Sagemaker*",
    "arn:aws:iam::*:role/*sagemaker*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "iot.amazonaws.com",
        "credentials.iot.amazonaws.com"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerFeatureStoreAccess

AmazonSageMakerFeatureStoreAccess est une [politique AWS gérée](#) qui : fournit les autorisations requises pour activer la boutique hors ligne pour un groupe de SageMaker FeatureStore fonctionnalités Amazon.

Utilisation de cette stratégie

Vous pouvez `AmazonSageMakerFeatureStoreAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 décembre 2020, 16:24 UTC
- Heure modifiée : 5 décembre 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
```



```
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*SageMaker*/metadata/*",
      "arn:aws:s3:::*Sagemaker*/metadata/*",
      "arn:aws:s3:::*sagemaker*/metadata/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:GetTable",
      "glue:UpdateTable"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/sagemaker_featurestore",
      "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerFullAccess

AmazonSageMakerFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon SageMaker via le SDK AWS Management Console and. Fournit également un accès sélectif aux services connexes (par exemple, S3, ECR, CloudWatch Logs).

Utilisation de cette politique

Vous pouvez vous associer AmazonSageMakerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 13:07 UTC
- Heure modifiée : 30 novembre 2023, 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Version de la politique

Version de la politique : v25 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:app/*"
    ]
  },
  {
    "Sid" : "AllowStudioActions",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreatePresignedDomainUrl",
      "sagemaker:DescribeDomain",
      "sagemaker:ListDomains",
      "sagemaker:DescribeUserProfile",
      "sagemaker:ListUserProfiles",
      "sagemaker:DescribeSpace",
      "sagemaker:ListSpaces",
      "sagemaker:DescribeApp",
      "sagemaker:ListApps"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAppActionsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  },
  {
    "Sid" : "AllowAppActionsForSharedSpaces",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition" : {

```

```

    "StringEquals" : {
      "sagemaker:SpaceSharingType" : [
        "Shared"
      ]
    }
  },
  {
    "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker:UpdateSpace",
      "sagemaker>DeleteSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  },
  {
    "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker:UpdateSpace",
      "sagemaker>DeleteSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private",
          "Shared"
        ]
      }
    }
  }
},

```

```

{
  "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateApp",
    "sagemaker>DeleteApp"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
  "Condition" : {
    "ArnLike" : {
      "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals" : {
      "sagemaker:SpaceSharingType" : [
        "Private"
      ]
    }
  }
},
{
  "Sid" : "AllowFlowDefinitionActions",
  "Effect" : "Allow",
  "Action" : "sagemaker:*",
  "Resource" : [
    "arn:aws:sagemaker:*:*:flow-definition/*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "sagemaker:WorkteamType" : [
        "private-crowd",
        "vendor-crowd"
      ]
    }
  }
},
{
  "Sid" : "AllowAWSServiceActions",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling>DeleteScalingPolicy",
    "application-autoscaling>DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",

```

```
"application-autoscaling:DescribeScalingActivities",
"application-autoscaling:DescribeScalingPolicies",
"application-autoscaling:DescribeScheduledActions",
"application-autoscaling:PutScalingPolicy",
"application-autoscaling:PutScheduledAction",
"application-autoscaling:RegisterScalableTarget",
"aws-marketplace:ViewSubscriptions",
"cloudformation:GetTemplateSummary",
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:PutMetricAlarm",
"cloudwatch:PutMetricData",
"codecommit:BatchGetRepositories",
"codecommit:CreateRepository",
"codecommit:GetRepository",
"codecommit:List*",
"cognito-idp:AdminAddUserToGroup",
"cognito-idp:AdminCreateUser",
"cognito-idp:AdminDeleteUser",
"cognito-idp:AdminDisableUser",
"cognito-idp:AdminEnableUser",
"cognito-idp:AdminRemoveUserFromGroup",
"cognito-idp:CreateGroup",
"cognito-idp:CreateUserPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp:CreateUserPoolDomain",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:List*",
"cognito-idp:UpdateUserPool",
"cognito-idp:UpdateUserPoolClient",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateVpcEndpoint",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
```

```
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:CreateRepository",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:StartImageScan",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"fsx:DescribeFileSystems",
"glue:CreateJob",
"glue>DeleteJob",
"glue:GetJob*",
"glue:GetTable*",
"glue:GetWorkflowRun",
"glue:ResetJobBookmark",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:UpdateJob",
"groundtruthlabeling:*",
"iam:ListRoles",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogDelivery",
"logs:Describe*",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:PutResourcePolicy",
"logs:UpdateLogDelivery",
"robomaker:CreateSimulationApplication",
"robomaker:DescribeSimulationApplication",
"robomaker>DeleteSimulationApplication",
"robomaker:CreateSimulationJob",
"robomaker:DescribeSimulationJob",
"robomaker:CancelSimulationJob",
```

```

    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowECRActions",
  "Effect" : "Allow",
  "Action" : [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr>DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr>DeleteRepository",
    "ecr:PutImage"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/*sagemaker*"
  ]
},
{
  "Sid" : "AllowCodeCommitActions",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:GitPull",
    "codecommit:GitPush"
  ],
  "Resource" : [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
  ]
},
{
  "Sid" : "AllowCodeBuildActions",
  "Action" : [

```



```

    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowStepFunctionsActions",
  "Action" : [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
    "arn:aws:states:*:*:execution:*sagemaker*:*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowSecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
  ]
},
{
  "Sid" : "AllowReadOnlySecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "*",

```

```

    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/SageMaker" : "true"
      }
    }
  },
  {
    "Sid" : "AllowServiceCatalogProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:ProvisionProduct"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:TerminateProvisionedProduct",
      "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "servicecatalog:userLevel" : "self"
      }
    }
  },
  {
    "Sid" : "AllowS3ObjectActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*",
      "arn:aws:s3::*aws-glue*"
    ]
  },
},

```

```
{
  "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*"
  ],
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/SageMaker" : "true"
    }
  }
},
{
  "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*"
  ],
  "Condition" : {
    "StringEquals" : {
      "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
    }
  }
},
{
  "Sid" : "AllowS3BucketActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors"
  ],
  "Resource" : "*"
},
{
```

```

    "Sid" : "AllowS3BucketACL",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketAcl",
      "s3:PutObjectAcl"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Sid" : "AllowLambdaInvokeFunction",
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda::*:function:*SageMaker*",
      "arn:aws:lambda::*:function:*sagemaker*",
      "arn:aws:lambda::*:function:*Sagemaker*",
      "arn:aws:lambda::*:function:*LabelingFunction*"
    ]
  },
  {
    "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {

```

```
        "iam:AWSServiceName" : "robomaker.amazonaws.com"
    }
}
},
{
    "Sid" : "AllowSNSActions",
    "Effect" : "Allow",
    "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
    ],
    "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
    ]
},
{
    "Sid" : "AllowPassRoleForSageMakerRoles",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "glue.amazonaws.com",
                "robomaker.amazonaws.com",
                "states.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AllowPassRoleToSageMaker",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
        "StringEquals" : {
```

```
        "iam:PassedToService" : "sagemaker.amazonaws.com"
    }
}
},
{
    "Sid" : "AllowAthenaActions",
    "Effect" : "Allow",
    "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "AllowGlueCreateTable",
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
    ]
},
{
    "Sid" : "AllowGlueUpdateTable",
    "Effect" : "Allow",
    "Action" : [
        "glue:UpdateTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
    ]
}
```

```
},
{
  "Sid" : "AllowGlueDeleteTable",
  "Effect" : "Allow",
  "Action" : [
    "glue:DeleteTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "AllowGlueGetTablesAndDatabases",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "AllowGlueGetAndCreateDatabase",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue:GetDatabase"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/sagemaker_featurestore",
    "arn:aws:glue:*:*:database/sagemaker_processing",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
  ]
},
{
  "Sid" : "AllowRedshiftDataActions",
```

```

    "Effect" : "Allow",
    "Action" : [
      "redshift-data:ExecuteStatement",
      "redshift-data:DescribeStatement",
      "redshift-data:CancelStatement",
      "redshift-data:GetStatementResult",
      "redshift-data:ListSchemas",
      "redshift-data:ListTables"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowRedshiftGetClusterCredentials",
    "Effect" : "Allow",
    "Action" : [
      "redshift:GetClusterCredentials"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
      "arn:aws:redshift:*:*:dbname:*"
    ]
  },
  {
    "Sid" : "AllowListTagsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:ListTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:user-profile/*"
    ]
  },
  {
    "Sid" : "AllowCloudformationListStackResources",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStackResources"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
  },
  {
    "Sid" : "AllowS3ExpressObjectActions",

```



```

    "Effect" : "Allow",
    "Action" : [
      "s3express:CreateSession"
    ],
    "Resource" : [
      "arn:aws:s3express:*:*:bucket/*SageMaker*",
      "arn:aws:s3express:*:*:bucket/*Sagemaker*",
      "arn:aws:s3express:*:*:bucket/*sagemaker*",
      "arn:aws:s3express:*:*:bucket/*aws-gluue*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AllowS3ExpressCreateBucketActions",
    "Effect" : "Allow",
    "Action" : [
      "s3express:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3express:*:*:bucket/*SageMaker*",
      "arn:aws:s3express:*:*:bucket/*Sagemaker*",
      "arn:aws:s3express:*:*:bucket/*sagemaker*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AllowS3ExpressListBucketActions",
    "Effect" : "Allow",
    "Action" : [
      "s3express:ListAllMyDirectoryBuckets"
    ],
    "Resource" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSageMakerGeospatialExecutionRole

AmazonSageMakerGeospatialExecutionRole est une [politique AWS gérée](#) qui : Cette politique fournit un accès aux services couramment nécessaires à l'utilisation de la SageMaker géospatiale.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerGeospatialExecutionRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 30 novembre 2022, 10:08 UTC
- Heure modifiée : 10 mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:PutObject",
      "s3:GetObject",
      "s3:ListBucketMultipartUploads"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "sagemaker-geospatial:GetEarthObservationJob",
    "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "sagemaker-geospatial:GetRasterDataCollection",
    "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerGeospatialFullAccess

AmazonSageMakerGeospatialFullAccess est une [stratégie AWS gérée](#) qui : Cette politique accorde des autorisations qui permettent un accès complet à Amazon SageMaker geospatial via la AWS Management Console et le kit SDK.

Utilisation de cette politique

Vous pouvez les associer `AmazonSageMakerGeospatialFullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 30 novembre 2022, 10:06 UTC
- Heure modifiée : 30 novembre 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
```

```
        "iam:PassedToService" : [  
            "sagemaker-geospatial.amazonaws.com"  
        ]  
    }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution est une [politiqueAWS gérée](#) qui : Fournit l'accès auxAWS services nécessaires à l'exécution de la tâche d' SageMaker GroundTruth étiquetage

Utilisation de cette stratégie

Vous pouvez les associerAmazonSageMakerGroundTruthExecution à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 09 juillet 2020, 19h30 UTC
- Heure modifiée : 29 avril 2022, 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3::*GroundTruth*",
        "arn:aws:s3::*Groundtruth*",
        "arn:aws:s3::*groundtruth*",
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData",
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "StreamingQueue",
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs:DeleteMessage",
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl",
      "sqs:ReceiveMessage",
      "sqs:SendMessage",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
  },
  {
    "Sid" : "StreamingTopicSubscribe",
```

```

"Effect" : "Allow",
"Action" : "sns:Subscribe",
"Resource" : [
  "arn:aws:sns:*:*:*GroundTruth*",
  "arn:aws:sns:*:*:*Groundtruth*",
  "arn:aws:sns:*:*:*groundTruth*",
  "arn:aws:sns:*:*:*groundtruth*",
  "arn:aws:sns:*:*:*SageMaker*",
  "arn:aws:sns:*:*:*Sagemaker*",
  "arn:aws:sns:*:*:*sageMaker*",
  "arn:aws:sns:*:*:*sagemaker*"
],
"Condition" : {
  "StringEquals" : {
    "sns:Protocol" : "sqs"
  },
  "StringLike" : {
    "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
  }
}
},
{
  "Sid" : "StreamingTopic",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:*GroundTruth*",
    "arn:aws:sns:*:*:*Groundtruth*",
    "arn:aws:sns:*:*:*groundTruth*",
    "arn:aws:sns:*:*:*groundtruth*",
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sageMaker*",
    "arn:aws:sns:*:*:*sagemaker*"
  ]
},
{
  "Sid" : "StreamingTopicUnsubscribe",
  "Effect" : "Allow",
  "Action" : [
    "sns:Unsubscribe"
  ],

```



```
    "Resource" : "*"
  },
  {
    "Sid" : "WorkforceVPC",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2:DescribeVpcEndpoints",
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ec2:VpceServiceName" : [
          "*sagemaker-task-resources*",
          "aws.sagemaker*labeling*"
        ]
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerMechanicalTurkAccess

AmazonSageMakerMechanicalTurkAccess est une [politique AWS gérée](#) qui : permet de créer des FlowDefinition ressources Amazon Augmented AI pour n'importe quelle équipe de travail.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerMechanicalTurkAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 16:19 UTC
- Heure modifiée : 3 décembre 2019, 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerModelGovernanceUseAccess

AmazonSageMakerModelGovernanceUseAccess est un [AWS politique gérée](#) : Ceci AWS la politique gérée accorde les autorisations nécessaires pour utiliser l'intégralité d'AmazonSageMaker Fonctionnalités de gouvernance. La politique fournit également un accès sélectionné aux services associés (par exemple, S3, KMS).

Utilisation de cette politique

Vous pouvez joindre AmazonSageMakerModelGovernanceUseAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 30 novembre 2022, 08:58 UTC
- Heure de modification : 17 juillet 2023, 22h31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
```

```

    "sagemaker:StopMonitoringSchedule",
    "sagemaker:ListMonitoringAlertHistory",
    "sagemaker:DescribeModelPackage",
    "sagemaker:DescribeModelPackageGroup",
    "sagemaker:CreateModelCard",
    "sagemaker:DescribeModelCard",
    "sagemaker:UpdateModelCard",
    "sagemaker>DeleteModelCard",
    "sagemaker:ListModelCards",
    "sagemaker:ListModelCardVersions",
    "sagemaker>CreateModelCardExportJob",
    "sagemaker:DescribeModelCardExportJob",
    "sagemaker:ListModelCardExportJobs"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTrainingJobs",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:ListModels",
    "sagemaker:DescribeModel",
    "sagemaker:Search",
    "sagemaker:AddTags",
    "sagemaker>DeleteTags",
    "sagemaker:ListTags"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:CreateBucket",
    "s3:GetBucketLocation"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccess est une [politique AWS gérée](#) qui : Il s'agit d'une nouvelle politique gérée pour Model Registry dans Sagemaker. Cette politique est une politique autonome qui peut être associée au rôle d'utilisateur pour accéder aux fonctionnalités liées au registre des modèles dans Sagemaker.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerModelRegistryFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 avril 2023, 05:20 UTC
- Heure modifiée : 13 avril 2023, 05:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "sagemaker:AddTags",
  "sagemaker:CreateModel",
  "sagemaker:CreateModelPackage",
  "sagemaker:CreateModelPackageGroup",
  "sagemaker:CreateEndpoint",
  "sagemaker:CreateEndpointConfig",
  "sagemaker:CreateInferenceRecommendationsJob",
  "sagemaker>DeleteModelPackage",
  "sagemaker>DeleteModelPackageGroup",
  "sagemaker>DeleteTags",
  "sagemaker:UpdateModelPackage"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*SageMaker*",
    "arn:aws:s3:::*Sagemaker*",
    "arn:aws:s3:::*sagemaker*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:DescribeImages"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
```

```

    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:GetGroupQuery"
    ],
    "Resource" : "arn:aws:resource-groups::*:group/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:Tag"
    ],
    "Resource" : "arn:aws:resource-groups::*:group/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "sagemaker:collection"
      }
    }
  }
},

```



```
{
  "Effect" : "Allow",
  "Action" : "resource-groups:DeleteGroup",
  "Resource" : "arn:aws:resource-groups:*:*:group/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:collection" : "true"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerNotebooksServiceRolePolicy

AmazonSageMakerNotebooksServiceRolePolicy est une [stratégie AWS gérée](#) qui : Stratégie gérée pour le rôle lié à un service pour Amazon SageMaker Notebooks

Utilisation de cette politique de politique en

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à ce service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles à vos rôles à vos utilisateurs, les groupes ou les rôles de ces stratégies

détails détails détails détails détails

- Type : Politique de rôles liée à un service
- Heure de création : 18 octobre 2019, 20:27 UTC
- Heure modifiée : 09 mars 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version par défaut de la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem>DeleteFileSystem",
    "elasticfilesystem>DeleteMountTarget"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticfilesystem:TagResource",
  "Resource" : [
    "arn:aws:elasticfilesystem:*:*:access-point/*",
    "arn:aws:elasticfilesystem:*:*:file-system/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
```

```

    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteManagedApplicationInstance",
    "sso:GetManagedApplicationInstance"
  ],
  "Resource" : "*"
}

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées stratégies gérées et évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège.](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy est un [AWS politique gérée](#) qui : politique de rôle de service utilisée par AWS Passerelle API au sein du AWS Service Catalog produits approvisionnés par Amazon SageMaker portefeuille de produits. Accorde des autorisations à un ensemble de services connexes, dont Lambda et d'autres.

Utilisation de cette politique

Vous pouvez

joindre AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 1 août 2023, 15:06 UTC
- Heure modifiée : 1 août 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicyest un[AWSpolitique gérée](#)qui : politique de rôle de service utilisée parAWS CloudFormationau sein duAWS ServiceCatalogproduits approvisionnés par AmazonSageMakerportefeuille de produits. Accorde des autorisations à un sous-ensemble de services connexes, notamment Lambda, ApiGateway et d'autres.

Utilisation de cette politique

Vous pouvez

joindreAmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicyà vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 1 août 2023, 15:06 UTC
- Heure de modification :1 août 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
```



```
    "lambda:UpdateFunctionCode",
    "lambda:ListTags",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:TagResource"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name",
        "sagemaker:partner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:PublishLayerVersion",
    "lambda:GetLayerVersion",
    "lambda>DeleteLayerVersion",
    "lambda:GetFunction"
  ],
}
```

```
"Resource" : [
  "arn:aws:lambda:*:*:layer:sagemaker-*",
  "arn:aws:lambda:*:*:function:sagemaker-*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET",
    "apigateway:DELETE",
    "apigateway:PATCH",
    "apigateway:POST",
    "apigateway:PUT"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/restapis/*",
    "arn:aws:apigateway:*:*/restapis"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:POST",
    "apigateway:PUT"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name",
        "sagemaker:partner"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy est un [AWS politique gérée](#) qui : politique de rôle de service utilisée par AWS Lambda au sein du AWS Service Catalog produits approvisionnés par Amazon SageMaker portefeuille de produits. Accorde des autorisations à un ensemble de services connexes, y compris Secrets Manager et d'autres.

Utilisation de cette politique

Vous pouvez

joindre `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 1 août 2023, 15:05 UTC
- Heure de modification : 1 août 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonSageMakerPipelinesIntegrations

AmazonSageMakerPipelinesIntegrationsest une [politiqueAWS gérée](#) qui : Cette politique gérée par Amazon accorde les autorisations généralement nécessaires pour une utilisation avec les étapes de rappel et les étapes Lambda dans les pipelines de création de SageMaker modèles. Il est ajouté au AmazonSageMaker -ExecutionRole qui peut être créé lors de la configuration de SageMaker Studio. Il peut également être attaché à n'importe quel autre rôle qui sera utilisé pour la création ou l'exécution de pipelines.

Utilisation de cette politique

Vous pouvez les associerAmazonSageMakerPipelinesIntegrations à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 juillet 2021, 16:35 UTC
- Heure modifiée : 17 février 2023, 21:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam:*:*:role/*",
      "Condition" : {
```

```

    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "elasticmapreduce.amazonaws.com",
        "ec2.amazonaws.com"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutRule",
      "events:PutTargets"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:AddJobFlowSteps",
      "elasticmapreduce:CancelSteps",
      "elasticmapreduce:DescribeStep",
      "elasticmapreduce:RunJobFlow",
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:TerminateJobFlows",
      "elasticmapreduce:ListSteps"
    ],
    "Resource" : [
      "arn:aws:elasticmapreduce:*:*:cluster/*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerReadOnly

AmazonSageMakerReadOnly est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon SageMaker via le SDKAWS Management Console et.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2017, 13:07 UTC
- Heure modifiée : 01 décembre 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```



```

    "sagemaker:List*",
    "sagemaker:BatchGetMetrics",
    "sagemaker:GetDeviceRegistration",
    "sagemaker:GetDeviceFleetReport",
    "sagemaker:GetSearchSuggestions",
    "sagemaker:BatchGetRecord",
    "sagemaker:GetRecord",
    "sagemaker:Search",
    "sagemaker:QueryLineage",
    "sagemaker:GetLineageGroupPolicy",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:GetModelPackageGroupPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "aws-marketplace:ViewSubscriptions",
    "cloudwatch:DescribeAlarms",
    "cognito-idp:DescribeUserPool",
    "cognito-idp:DescribeUserPoolClient",
    "cognito-idp:ListGroups",
    "cognito-idp:ListIdentityProviders",
    "cognito-idp:ListUserPoolClients",
    "cognito-idp:ListUserPools",
    "cognito-idp:ListUsers",
    "cognito-idp:ListUsersInGroup",
    "ecr:Describe*"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy est une [politique AWS gérée](#) qui : Politique de rôle de service utilisée par AWS ApiGateway dans les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes, y compris CloudWatch les journaux et autres.

Utilisation de cette stratégie

Vous pouvez AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 25 mars 2022, 04:25 UTC
- Heure modifiée : 25 mars 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs>DeleteLogDelivery",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:DescribeResourcePolicies",
      "logs:DescribeDestinations",
      "logs:DescribeExportTasks",
      "logs:DescribeMetricFilters",
      "logs:DescribeQueries",
      "logs:DescribeQueryDefinitions",
      "logs:DescribeSubscriptionFilters",
      "logs:GetLogDelivery",
      "logs:GetLogEvents",
      "logs:PutLogEvents",
      "logs:PutResourcePolicy",
      "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy est une [politique AWS gérée](#) qui : Politique de rôle de service utilisée par AWS CloudFormation les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon.

Accorde des autorisations à un sous-ensemble de services connexes, y compris SageMaker et d'autres.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 25 mars 2022, 04:26 UTC
- Heure modifiée : 25 mars 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
```

```
"sagemaker:CreateAction",
"sagemaker:CreateAlgorithm",
"sagemaker:CreateApp",
"sagemaker:CreateAppImageConfig",
"sagemaker:CreateArtifact",
"sagemaker:CreateAutoMLJob",
"sagemaker:CreateCodeRepository",
"sagemaker:CreateCompilationJob",
"sagemaker:CreateContext",
"sagemaker:CreateDataQualityJobDefinition",
"sagemaker:CreateDeviceFleet",
"sagemaker:CreateDomain",
"sagemaker:CreateEdgePackagingJob",
"sagemaker:CreateEndpoint",
"sagemaker:CreateEndpointConfig",
"sagemaker:CreateExperiment",
"sagemaker:CreateFeatureGroup",
"sagemaker:CreateFlowDefinition",
"sagemaker:CreateHumanTaskUi",
"sagemaker:CreateHyperParameterTuningJob",
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
```

```
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
"sagemaker>DeleteModelPackageGroup",
"sagemaker>DeleteModelPackageGroupPolicy",
"sagemaker>DeleteModelQualityJobDefinition",
"sagemaker>DeleteMonitoringSchedule",
"sagemaker>DeleteNotebookInstance",
"sagemaker>DeleteNotebookInstanceLifecycleConfig",
"sagemaker>DeletePipeline",
"sagemaker>DeleteProject",
"sagemaker>DeleteRecord",
"sagemaker>DeleteTags",
"sagemaker>DeleteTrial",
"sagemaker>DeleteTrialComponent",
"sagemaker>DeleteUserProfile",
"sagemaker>DeleteWorkforce",
"sagemaker>DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
```

```
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
```

```
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
```



```
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
```

```
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"NotResource" : [
  "arn:aws:sagemaker:*:*:domain/*",
  "arn:aws:sagemaker:*:*:user-profile/*",
  "arn:aws:sagemaker:*:*:app/*",
  "arn:aws:sagemaker:*:*:flow-definition/*"
]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy est une [politique AWS gérée](#) qui : Politique de rôle de service utilisée par AWS CodeBuild les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un sous-ensemble de services CodeBuild connexes CodePipeline, notamment.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 25 mars 2022, 04:27 UTC
- Heure modifiée : 25 mars 2022, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:CompleteLayerUpload",
      "ecr:CreateRepository",
      "ecr:InitiateLayerUpload",
      "ecr:PutImage",
      "ecr:UploadLayerPart"
    ],
    "Resource" : [
      "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "events.amazonaws.com",
          "codepipeline.amazonaws.com",
          "cloudformation.amazonaws.com",
          "codebuild.amazonaws.com",
          "sagemaker.amazonaws.com"
        ]
      }
    }
  }
]

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:DescribeResourcePolicies",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeMetricFilters",
    "logs:DescribeQueries",
    "logs:DescribeQueryDefinitions",
    "logs:DescribeSubscriptionFilters",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:PutBucketCors",
    "s3:AbortMultipartUpload",
    "s3>DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
```

```
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
    "sagemaker:CreateAction",
    "sagemaker:CreateAlgorithm",
    "sagemaker:CreateApp",
    "sagemaker:CreateAppImageConfig",
    "sagemaker:CreateArtifact",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateCodeRepository",
    "sagemaker:CreateCompilationJob",
    "sagemaker:CreateContext",
    "sagemaker:CreateDataQualityJobDefinition",
    "sagemaker:CreateDeviceFleet",
    "sagemaker:CreateDomain",
    "sagemaker:CreateEdgePackagingJob",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateExperiment",
    "sagemaker:CreateFeatureGroup",
    "sagemaker:CreateFlowDefinition",
    "sagemaker:CreateHumanTaskUi",
    "sagemaker:CreateHyperParameterTuningJob",
    "sagemaker:CreateImage",
    "sagemaker:CreateImageVersion",
    "sagemaker:CreateInferenceRecommendationsJob",
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateLineageGroupPolicy",
    "sagemaker:CreateModel",
    "sagemaker:CreateModelBiasJobDefinition",
```

```
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
```



```
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
```

```
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
```

```
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
```

```
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
```

```

    "sagemaker:UpdateNotebookInstanceLifecycleConfig",
    "sagemaker:UpdatePipeline",
    "sagemaker:UpdatePipelineExecution",
    "sagemaker:UpdateProject",
    "sagemaker:UpdateTrainingJob",
    "sagemaker:UpdateTrial",
    "sagemaker:UpdateTrialComponent",
    "sagemaker:UpdateUserProfile",
    "sagemaker:UpdateWorkforce",
    "sagemaker:UpdateWorkteam"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:endpoint/*",
    "arn:aws:sagemaker:*:*:endpoint-config/*",
    "arn:aws:sagemaker:*:*:model/*",
    "arn:aws:sagemaker:*:*:pipeline/*",
    "arn:aws:sagemaker:*:*:project/*",
    "arn:aws:sagemaker:*:*:model-package/*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy est une [politique AWS gérée](#) qui : Politique de rôle de service utilisée par AWS CodePipeline les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un sous-ensemble de services CodeBuild connexes CodePipeline, notamment.

Utilisation de cette stratégie

Vous

pouvez associer `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` les utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 22 février 2022, 09:53 UTC
- Heure modifiée : 22 février 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ]
    }
  ],
}
```

```

    "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "codebuild:BatchGetBuilds",
      "codebuild:StartBuild"
    ],
    "Resource" : [
      "arn:aws:codebuild:*:*:project/sagemaker-*",
      "arn:aws:codebuild:*:*:build/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "codecommit:CancelUploadArchive",
      "codecommit:GetBranch",
      "codecommit:GetCommit",
      "codecommit:GetUploadArchiveStatus",
      "codecommit:UploadArchive"
    ]
  }

```

```
    ],  
    "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle de service utilisée par les AWS CloudWatch événements au sein des produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un sous-ensemble de services connexes, y compris CodePipeline et d'autres.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 22 février 2022, 09:53 UTC
- Heure modifiée : 22 février 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle de service utilisée par AWS Firehose dans le cadre des produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes, notamment Firehose.

Utilisation de cette stratégie

Vous pouvez AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 22 février 2022, 09:54 UTC
- Heure modifiée : 22 février 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle de service utilisée par AWS Glue dans les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes, notamment Glue, S3 et autres.

Utilisation de cette stratégie

Vous pouvez AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 22 février 2022, 09:51 UTC
- Heure modifiée : 26 août 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
```

```

    "glue:BatchDeleteTableVersion",
    "glue:BatchGetPartition",
    "glue:CreateDatabase",
    "glue:CreatePartition",
    "glue:CreateTable",
    "glue>DeletePartition",
    "glue>DeleteTable",
    "glue>DeleteTableVersion",
    "glue:GetDatabase",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetTableVersion",
    "glue:GetTableVersions",
    "glue:SearchTables",
    "glue:UpdatePartition",
    "glue:UpdateTable",
    "glue:GetUserDefinedFunctions"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:database/global_temp",
    "arn:aws:glue:*:*:database/sagemaker-*",
    "arn:aws:glue:*:*:table/sagemaker-*",
    "arn:aws:glue:*:*:tableVersion/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3>ListAllMyBuckets",
    "s3>ListBucket",
    "s3>ListBucketMultipartUploads",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",

```

```
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle de service utilisée par AWS Lambda dans les produits AWS ServiceCatalog provisionnés à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes, notamment ECR, S3 et autres.

Utilisation de cette stratégie

Vous pouvez AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 4 avril 2022, 16:34 UTC
- Heure modifiée : 4 avril 2022, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "ecr:DescribeImages",
    "ecr:BatchDeleteImage",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr>DeleteRepository",
    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3>ListAllMyBuckets",
    "s3>ListBucket",
    "s3>ListBucketMultipartUploads",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
    "sagemaker:CreateAction",
    "sagemaker:CreateAlgorithm",
    "sagemaker:CreateApp",
    "sagemaker:CreateAppImageConfig",
    "sagemaker:CreateArtifact",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateCodeRepository",
    "sagemaker:CreateCompilationJob",
    "sagemaker:CreateContext",
    "sagemaker:CreateDataQualityJobDefinition",
    "sagemaker:CreateDeviceFleet",
    "sagemaker:CreateDomain",
    "sagemaker:CreateEdgePackagingJob",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateExperiment",
    "sagemaker:CreateFeatureGroup",
    "sagemaker:CreateFlowDefinition",
    "sagemaker:CreateHumanTaskUi",
    "sagemaker:CreateHyperParameterTuningJob",
```



```
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
```

```
"sagemaker:DeleteImage",
"sagemaker:DeleteImageVersion",
"sagemaker:DeleteLineageGroupPolicy",
"sagemaker:DeleteModel",
"sagemaker:DeleteModelBiasJobDefinition",
"sagemaker:DeleteModelExplainabilityJobDefinition",
"sagemaker:DeleteModelPackage",
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
```

```
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
```

```
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker: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/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:DescribeResourcePolicies",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeMetricFilters",
    "logs:DescribeQueries",
    "logs:DescribeQueryDefinitions",

```

```
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSecurityLakeAdministrator

AmazonSecurityLakeAdministrator est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Security Lake et aux services associés nécessaires à l'administration de Security Lake.

Utilisation de cette politique

Vous pouvez vous associer AmazonSecurityLakeAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2023, 22:04 UTC
- Heure modifiée : 23 février 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowManagingSecurityLakeS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ],
    "Resource" : "arn:aws:s3:::aws-security-data-lake*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowLambdaCreateFunction",
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {

```

```
        "aws:CalledVia" : "securitylake.amazonaws.com"
    }
}
},
{
    "Sid" : "AllowLambdaAddPermission",
    "Effect" : "Allow",
    "Action" : [
        "lambda:AddPermission"
    ],
    "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
            "lambda:Principal" : "securitylake.amazonaws.com"
        }
    }
}
},
{
    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
}
},
{
```

```

    "Sid" : "AllowEventBridgeActions",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
      "events>DeleteConnection",
      "events>DeleteApiDestination",
      "events:ListTargetsByRule",
      "events:RemoveTargets",
      "events>DeleteRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/AmazonSecurityLake*",
      "arn:aws:events:*:*:rule/SecurityLake*",
      "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
      "arn:aws:events:*:*:connection/AmazonSecurityLake*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowSQSActions",
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes",
      "sqs:GetQueueURL",
      "sqs:AddPermission",
      "sqs:GetQueueAttributes",
      "sqs>DeleteQueue"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:SecurityLake*",
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition" : {

```

```

    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  },
  {
    "Sid" : "AllowKmsCmkGrantForSecurityLake",
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      },
      "StringLike" : {
        "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals" : {
        "kms:GrantOperations" : [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid" : "AllowEnablingQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ram:ResourceArn" : [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      }
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
}

```

```

    }
  },
  {
    "Sid" : "AllowConfiguringQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram>DeleteResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : "LakeFormation*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",

```

```

    "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
    }
  }
},
{
  "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
    "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ]
    }
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "securitylake.amazonaws.com"
  }
}
},
{
  "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "s3.amazonaws.com"
    }
  },

```

```

    "StringLike" : {
      "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
    }
  },
  {
    "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "s3.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:s3::*:aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",

```



```

    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "events.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "events.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowOnboardingToSecurityLakeDependencies",

```

```

    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinations.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AllowRolePolicyActionsforSubscribersandSources",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition" : {
      "StringEquals" : {
        "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowRegisterS3LocationInLakeFormation",
    "Effect" : "Allow",
    "Action" : [
      "iam:PutRolePolicy",

```

```

    "iam:GetRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowIAMActionsByResource",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRolePolicies",
    "iam>DeleteRole"
  ],
  "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "S3ReadAccessToSecurityLakes",
  "Effect" : "Allow",
  "Action" : [
    "s3:Get*",
    "s3:List*"
  ],
  "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
},
{
  "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
},
{
  "Sid" : "S3ResourcelessReadOnly",

```

```
    "Effect" : "Allow",
    "Action" : [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSecurityLakeMetastoreManager

AmazonSecurityLakeMetastoreManager est une [politique AWS gérée qui : Politique](#) pour le gestionnaire de SecurityLake méta-boutiques Amazon Lambda qui autorise l'accès à Cloudwatch, S3, Glue et SQS.

Utilisation de cette politique

Vous pouvez vous associer AmazonSecurityLakeMetastoreManager à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 23 janvier 2024, 15:26 UTC
- Heure modifiée : 23 janvier 2024, 15:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*"
      ]
    }
  ]
}
```

```
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowToReadFromSqs",
  "Effect" : "Allow",
  "Action" : [
    "sqs:ReceiveMessage",
    "sqs>DeleteMessage",
    "sqs:GetQueueAttributes"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowMetaDataReadWrite",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-security-data-lake*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonSecurityLakePermissionsBoundary

AmazonSecurityLakePermissionsBoundary est une [politique AWS gérée](#) qui : Amazon Security Lake crée des rôles IAM pour des sources personnalisées tierces afin d'écrire des données dans un lac de données et pour des abonnés tiers afin de consommer des données provenant d'un lac de données, et utilise cette politique lors de la création de ces rôles pour définir les limites de leurs autorisations.

Utilisation de cette stratégie

Vous pouvez AmazonSecurityLakePermissionsBoundary les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2022, 14:11 UTC
- Heure modifiée : 29 novembre 2022, 14:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",

```



```
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation"
  ],
  "NotResource" : [
    "arn:aws:s3:::aws-security-data-lake*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com",
        "sqs.*.amazonaws.com"
      ]
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "kms:EncryptionContext:aws:s3:arn" : "false"
    },
    "StringNotLikeIfExists" : {
      "kms:EncryptionContext:aws:s3:arn" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "kms:EncryptionContext:aws:sqs:arn" : "false"
    },
    "StringNotLikeIfExists" : {
      "kms:EncryptionContext:aws:sqs:arn" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSESFu11Access

AmazonSESFu11Access est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon SES via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonSESFu11Access à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFu11Access`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "ses:*"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSESReadOnlyAccess

AmazonSESReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon SES via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAmazonSESReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSNSFullAccess

AmazonSNSFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon SNS via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AmazonSNSFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSNSReadOnlyAccess

AmazonSNSReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon SNS via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez `AmazonSNSReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSNSRole

AmazonSNSRole est une [politiqueAWS gérée qui : Politique](#) par défaut pour le rôle de service Amazon SNS.

Utilisation de cette stratégie

Vous pouvez AmazonSNSRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSQSFullAccess

AmazonSQSFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon SQS via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAmazonSQSFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSQSReadOnlyAccess

AmazonSQSReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon SQS via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez l'associer AmazonSQSReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 15 juin 2023, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess [AWS est une stratégie](#)

Using this policy

Vous pouvez les associer AmazonSSMAutomationApproverAccess à vos utilisateurs, à vos groupes et à vos rôles.

Policy details

- Type : politique AWS gérée
- Heure de création : 7 août 2017, 23:07 UTC
- Heure modifiée : 7 août 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    ]
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-attach-detach.html
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [DémarrerAWS](#)

AmazonSSMAutomationRole

AmazonSSMAutomationRoleest une [politiqueAWS gérée](#) qui : fournit des autorisations au service EC2 Automation pour exécuter les activités définies dans les documents d'automatisation

Utilisation de cette stratégie

Vous pouvezAmazonSSMAutomationRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 décembre 2016, 22:09 UTC
- Heure modifiée : 24 juillet 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2>DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "ssm:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:Automation*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMDirectoryServiceAccess

AmazonSSMDirectoryServiceAccess est une [politiqueAWS gérée](#) qui : Cette politique permet à l'agent SSM d'accéder au Directory Service au nom du client pour rejoindre le domaine de l'instance gérée.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSSMDirectoryServiceAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 15 mars 2019, 17:44 UTC
- Heure modifiée : 15 mars 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMFullAccess

AmazonSSMFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon SSM.

Utilisation de cette stratégie

Vous pouvez `AmazonSSMFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 mai 2015, 17:39 UTC
- Heure modifiée : 20 novembre 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole est une [politique AWS gérée](#) qui : Rôle de service à utiliser pour la fenêtre de maintenance EC2

Utilisation de cette stratégie

Vous pouvez AmazonSSMMaintenanceWindowRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2016, 15:57 UTC
- Heure modifiée : 27 juillet 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
```

```
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SSM*",
    "arn:aws:lambda:*:*:function:*:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states:DescribeExecution",
    "states:StartExecution"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:SSM*",
    "arn:aws:states:*:*:execution:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:ListGroup",
    "resource-groups:ListGroupResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSManagedEC2InstanceDefaultPolicy

AmazonSSManagedEC2InstanceDefaultPolicyest une [politiqueAWS gérée](#) qui : Cette politique activeAWS les fonctionnalités de Systems Manager sur les instances EC2.

Utilisation de cette stratégie

Vous pouvez les associerAmazonSSManagedEC2InstanceDefaultPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 août 2022, 20:54 UTC
- Heure modifiée : 30 août 2022, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSManagedEC2InstanceDefaultPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeAssociation",
      "ssm:GetDeployablePatchSnapshotForInstance",
      "ssm:GetDocument",
      "ssm:DescribeDocument",
      "ssm:GetManifest",
      "ssm:ListAssociations",
      "ssm:ListInstanceAssociations",
      "ssm:PutInventory",
      "ssm:PutComplianceItems",
      "ssm:PutConfigurePackageResult",
      "ssm:UpdateAssociationStatus",
      "ssm:UpdateInstanceAssociationStatus",
      "ssm:UpdateInstanceInformation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2messages:AcknowledgeMessage",
      "ec2messages:DeleteMessage",
      "ec2messages:FailMessage",
      "ec2messages:GetEndpoint",
      "ec2messages:GetMessages",
      "ec2messages:SendReply"
    ],
    "Resource" : "*"
  }
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMManagedInstanceCore

AmazonSSMManagedInstanceCore est une [politiqueAWS gérée](#) qui : La politique relative au rôle Amazon EC2 afin d'activerAWS les fonctionnalités de base du service Systems Manager.

Utilisation de cette stratégie

Vous pouvezAmazonSSMManagedInstanceCore les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 mars 2019, 17:22 UTC
- Heure modifiée : 23 mai 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeAssociation",
      "ssm:GetDeployablePatchSnapshotForInstance",
      "ssm:GetDocument",
      "ssm:DescribeDocument",
      "ssm:GetManifest",
      "ssm:GetParameter",
      "ssm:GetParameters",
      "ssm:ListAssociations",
      "ssm:ListInstanceAssociations",
      "ssm:PutInventory",
      "ssm:PutComplianceItems",
      "ssm:PutConfigurePackageResult",
      "ssm:UpdateAssociationStatus",
      "ssm:UpdateInstanceAssociationStatus",
      "ssm:UpdateInstanceInformation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2messages:AcknowledgeMessage",
      "ec2messages:DeleteMessage",
      "ec2messages:FailMessage",
      "ec2messages:GetEndpoint",
      "ec2messages:GetMessages",
      "ec2messages:SendReply"
    ],
    "Resource" : "*"
  }
]
```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMPatchAssociation

AmazonSSMPatchAssociation est une [politiqueAWS gérée](#) qui : fournit un accès aux instances enfants pour les opérations d'association de correctifs.

Utilisation de cette stratégie

Vous pouvez les associer AmazonSSMPatchAssociation à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 mai 2020, 16h00 UTC
- Heure modifiée : 13 mai 2020, 16 h 00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMReadOnlyAccess

AmazonSSMReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon SSM.

Utilisation de cette stratégie

Vous pouvez associer `AmazonSSMReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 mai 2015, 17:44 UTC
- Heure modifiée : 29 mai 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un accès aux AWS ressources gérées ou utilisées par Amazon SSM

Utilisation des politiques Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les stratégies de stratégies de stratégie de stratégie de stratégie de stratégie de

Détails des politiques des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 novembre 2017, 19:20 UTC
- Heure modifiée : 14 septembre 2022, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut des stratégies de stratégie est la version qui définit des autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)


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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTexttractFullAccess

AmazonTexttractFullAccess est une [politique AWS gérée](#) qui : Accès à toutes les API Amazon Texttract

Utilisation de cette stratégie

Vous pouvez AmazonTexttractFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 19:07 UTC
- Heure modifiée : 28 novembre 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTexttractFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTextextractServiceRole

AmazonTextextractServiceRole est une [politique AWS gérée](#) qui : Autorise Textract à appeler AWS des services en votre nom.

Utilisation de cette stratégie

Vous pouvez AmazonTextextractServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 28 novembre 2018, 19:12 UTC
- Heure modifiée : 28 novembre 2018, 19:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextextractServiceRole

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTimestreamConsoleFullAccess

AmazonTimestreamConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à la gestion d'Amazon Timestream à l'aide du AWS Management Console. Notez que cette politique accorde également des autorisations pour certaines opérations KMS et pour des opérations permettant de gérer vos requêtes enregistrées. Si vous utilisez une clé CMK gérée par le client, consultez la documentation pour connaître les autorisations supplémentaires nécessaires.

Utilisation de cette stratégie

Vous pouvez `AmazonTimestreamConsoleFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 1 février 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "kms:EncryptionContextKeys" : "aws:timestream:database-name"
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      },
      "StringLike" : {
        "kms:ViaService" : "timestream.*.amazonaws.com"
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "dbqms:CreateFavoriteQuery",
    "dbqms:DescribeFavoriteQueries",
    "dbqms:UpdateFavoriteQuery",
    "dbqms>DeleteFavoriteQueries",
    "dbqms:GetQueryString",
    "dbqms:CreateQueryHistory",
    "dbqms:DescribeQueryHistory",
    "dbqms:UpdateQueryHistory",
    "dbqms>DeleteQueryHistory"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
        "sns:ListTopics",
        "iam:ListRoles"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTimestreamFullAccess

AmazonTimestreamFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Timestream. Notez que cette politique accorde également l'accès à certaines opérations KMS. Si vous utilisez une clé CMK gérée par le client, consultez la documentation pour connaître les autorisations supplémentaires nécessaires.

Utilisation de cette stratégie

Vous pouvez AmazonTimestreamFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 26 novembre 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
```

```
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccess est une [politique AWS gérée](#) qui : fournit un accès administratif complet pour créer, mettre à jour, supprimer et répertorier les instances Amazon Timestream InfluxDB ainsi que pour créer et répertorier des groupes de paramètres. Reportez-vous à la documentation pour connaître les autorisations supplémentaires nécessaires.

Utilisation de cette politique

Vous pouvez vous associer AmazonTimestreamInfluxDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 mars 2024, 22:53 UTC
- Heure modifiée : 14 mars 2024, 22:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb>DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam:*:*:role/aws-service-role/timestream-influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "CreateEniInSubnetStatement",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "BucketValidationStatement",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketPolicy"
    ],
    "Resource" : [
      "arn:aws:s3::*:*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonTimestreamInfluxDBServiceRolePolicy

AmazonTimestreamInfluxDBServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un accès administratif complet pour créer, mettre à jour, supprimer et répertorier les instances Amazon Timestream InfluxDB ainsi que pour créer et répertorier des groupes de paramètres. Reportez-vous à la documentation pour connaître les autorisations supplémentaires nécessaires.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 14 mars 2024, 18:53 UTC
- Heure modifiée : 14 mars 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
```

```

    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
    },
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateNetworkInterface"
      ]
    }
  }
},
{
  "Sid" : "ManageEniStatement",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
    }
  }
},
{
  "Sid" : "PutCloudWatchMetricsStatement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Timestream/InfluxDB",
        "AWS/Usage"
      ]
    }
  }
},
  "Resource" : [
    "*"
  ]
}

```

```
    ]
  },
  {
    "Sid" : "ManageSecretStatement",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager>DeleteSecret"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Timestream. La politique fournit également l'autorisation d'annuler toute requête en cours d'exécution. Si vous utilisez une clé CMK gérée par le client, consultez la documentation pour connaître les autorisations supplémentaires nécessaires.

Utilisation de cette stratégie

Vous pouvez AmazonTimestreamReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 28 février 2023, 18:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTranscribeFullAccess

AmazonTranscribeFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux opérations Amazon Transcribe

Utilisation de cette stratégie

Vous pouvez les associer AmazonTranscribeFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 4 avril 2018, 16:06 UTC
- Heure modifiée : 4 avril 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*transcribe*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonTranscribeReadOnlyAccess

AmazonTranscribeReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit l'accès au fonctionnement en lecture seule pour Amazon Transcribe

Utilisation de cette stratégie

Vous pouvez `AmazonTranscribeReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 4 avril 2018, 16:05 UTC
- Heure modifiée : 4 avril 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations est une [politique AWS gérée](#) qui : fournit un accès pour créer des interfaces réseau et les associer à des ressources entre comptes

Utilisation de cette politique

Vous pouvez vous associer AmazonVPCCrossAccountNetworkInterfaceOperations à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juillet 2017, 20:47 UTC
- Heure modifiée : 25 septembre 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
    "ec2:DescribeRouteTables",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2:ReplaceRoute"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeNetworkInterfaces",
    "ec2:CreateNetworkInterface",
    "ec2>DeleteNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonVPCFullAccess

AmazonVPCFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon VPC via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonVPCFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 8 février 2024, 16:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```



```
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpcEndpointConnectionNotification",
"ec2:CreateVpcEndpointServiceConfiguration",
"ec2:CreateVpcPeeringConnection",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteCarrierGateway",
"ec2>DeleteCustomerGateway",
"ec2>DeleteDhcpOptions",
"ec2>DeleteEgressOnlyInternetGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteInternetGateway",
"ec2>DeleteLocalGatewayRouteTableVpcAssociation",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkAcl",
"ec2>DeleteNetworkAclEntry",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2>DeleteSecurityGroup",
"ec2>DeleteSubnet",
"ec2>DeleteTags",
"ec2>DeleteVpc",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteVpcEndpointConnectionNotifications",
"ec2>DeleteVpcEndpointServiceConfigurations",
"ec2>DeleteVpcPeeringConnection",
"ec2>DeleteVpnConnection",
"ec2>DeleteVpnConnectionRoute",
"ec2>DeleteVpnGateway",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeCustomerGateways",
```

```
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeIpv6Pools",
"ec2:DescribeLocalGatewayRouteTables",
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeKeyPairs",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DetachClassicLinkVpc",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLink",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
```

```

    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:DisassociateVpcCidrBlock",
    "ec2:EnableVgwRoutePropagation",
    "ec2:EnableVpcClassicLink",
    "ec2:EnableVpcClassicLinkDnsSupport",
    "ec2:GetSecurityGroupsForVpc",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifySecurityGroupRules",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ModifyVpcEndpoint",
    "ec2:ModifyVpcEndpointConnectionNotification",
    "ec2:ModifyVpcEndpointServiceConfiguration",
    "ec2:ModifyVpcEndpointServicePermissions",
    "ec2:ModifyVpcPeeringConnectionOptions",
    "ec2:ModifyVpcTenancy",
    "ec2:MoveAddressToVpc",
    "ec2:RejectVpcEndpointConnections",
    "ec2:RejectVpcPeeringConnection",
    "ec2:ReleaseAddress",
    "ec2:ReplaceNetworkAclAssociation",
    "ec2:ReplaceNetworkAclEntry",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:ResetNetworkInterfaceAttribute",
    "ec2:RestoreAddressToClassic",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:UnassignIpv6Addresses",
    "ec2:UnassignPrivateIpAddresses",
    "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
    "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy est une [politique AWS gérée](#) qui : fournit des autorisations pour décrire les AWS ressources, exécuter Network Access Analyzer et créer ou supprimer des balises sur Network Insights Access Scope et Network Insights Access Scope Analysis.

Utilisation de cette politique

Vous pouvez vous associer AmazonVPCNetworkAccessAnalyzerFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 juin 2023, 22:56 UTC
- Heure modifiée : 3 novembre 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Action" : [
  "directconnect:DescribeConnections",
  "directconnect:DescribeDirectConnectGatewayAssociations",
  "directconnect:DescribeDirectConnectGatewayAttachments",
  "directconnect:DescribeDirectConnectGateways",
  "directconnect:DescribeVirtualGateways",
  "directconnect:DescribeVirtualInterfaces"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInsightsAccessScope",
    "ec2>DeleteNetworkInsightsAccessScope",
    "ec2>DeleteNetworkInsightsAccessScopeAnalysis",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
    "ec2:DescribeNetworkInsightsAccessScopes",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
```

```
    "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
    "ec2:GetNetworkInsightsAccessScopeContent",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAccessScopeAnalysis"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-access-scope/*",
    "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

AmazonVPCReachabilityAnalyzerFullAccessPolicy est une [politique AWS gérée](#) qui : fournit des autorisations pour décrire les AWS ressources, exécuter Reachability Analyzer et créer ou supprimer des balises sur Network Insights Path et Network Insights Analysis.

Utilisation de cette politique

Vous pouvez vous associer AmazonVPCReachabilityAnalyzerFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 juin 2023, 20:12 UTC
- Heure modifiée : 3 novembre 2023, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



```

    "directconnect:DescribeConnections",
    "directconnect:DescribeDirectConnectGatewayAssociations",
    "directconnect:DescribeDirectConnectGatewayAttachments",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "directconnect:DescribeVirtualInterfaces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInsightsPath",
    "ec2>DeleteNetworkInsightsAnalysis",
    "ec2>DeleteNetworkInsightsPath",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAnalyses",
    "ec2:DescribeNetworkInsightsPaths",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
  ]
}

```

```

    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAnalysis"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-path/*",
    "arn:*:ec2:*:*:network-insights-analysis/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",

```

```
    "Action" : [
      "network-firewall:DescribeFirewall",
      "network-firewall:DescribeFirewallPolicy",
      "network-firewall:DescribeResourcePolicy",
      "network-firewall:DescribeRuleGroup",
      "network-firewall:ListFirewallPolicies",
      "network-firewall:ListFirewalls",
      "network-firewall:ListRuleGroups"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "tiros:CreateQuery",
      "tiros:ExtendQuery",
      "tiros:GetQueryAnswer",
      "tiros:GetQueryExplanation",
      "tiros:GetQueryExtensionAccounts"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy est une [politique AWS gérée](#) qui : Cette politique est attachée au rôle IAMRoleForReachabilityAnalyzerCrossAccountResource Access. Ce rôle est déployé sur les comptes des membres d'une organisation lorsque le compte de gestion autorise un accès sécurisé à Reachability Analyzer. Il fournit les autorisations nécessaires pour consulter les ressources de l'ensemble de votre organisation à l'aide de la console Reachability Analyzer.

Utilisation de cette stratégie

Vous pouvez les associer `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 mai 2023, 20:38 UTC
- Heure modifiée : 01 mai 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonVPCReadOnlyAccess

AmazonVPCReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon VPC via le AWS Management Console

Utilisation de cette politique

Vous pouvez vous associer AmazonVPCReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 8 février 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Sid" : "AmazonVPCReadOnlyAccess",
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAddresses",
  "ec2:DescribeCarrierGateways",
  "ec2:DescribeClassicLinkInstances",
  "ec2:DescribeCustomerGateways",
  "ec2:DescribeDhcpOptions",
  "ec2:DescribeEgressOnlyInternetGateways",
  "ec2:DescribeFlowLogs",
  "ec2:DescribeInternetGateways",
  "ec2:DescribeLocalGatewayRouteTables",
  "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
  "ec2:DescribeMovingAddresses",
  "ec2:DescribeNatGateways",
  "ec2:DescribeNetworkAcls",
  "ec2:DescribeNetworkInterfaceAttribute",
  "ec2:DescribeNetworkInterfacePermissions",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribePrefixLists",
  "ec2:DescribeRouteTables",
  "ec2:DescribeSecurityGroupReferences",
  "ec2:DescribeSecurityGroupRules",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeStaleSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeTags",
  "ec2:DescribeVpcAttribute",
  "ec2:DescribeVpcClassicLink",
  "ec2:DescribeVpcClassicLinkDnsSupport",
  "ec2:DescribeVpcEndpoints",
  "ec2:DescribeVpcEndpointConnectionNotifications",
  "ec2:DescribeVpcEndpointConnections",
  "ec2:DescribeVpcEndpointServiceConfigurations",
  "ec2:DescribeVpcEndpointServicePermissions",
  "ec2:DescribeVpcEndpointServices",
  "ec2:DescribeVpcPeeringConnections",
  "ec2:DescribeVpcs",
  "ec2:DescribeVpnConnections",
  "ec2:DescribeVpnGateways",
  "ec2:GetSecurityGroupsForVpc"
],
"Resource" : "*"

```

```
}  
 ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AmazonWorkDocsFullAccess

AmazonWorkDocsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon WorkDocs via AWS Management Console

Utilisation de cette stratégie

Vous pouvez AmazonWorkDocsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 16 avril 2020, 23:05 UTC
- Heure modifiée : 16 avril 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à Amazon WorkDocs viaAWS Management Console

Utilisation de cette stratégie

Vous pouvezAmazonWorkDocsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 janvier 2020, 23:49 UTC

- Heure modifiée : 8 janvier 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkMailEventsServiceRolePolicy

AmazonWorkMailEventsServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise l'accès Services AWS aux ressources utilisées ou gérées par Amazon WorkMail Events

Using this policy

Cette stratégie est attachée à un rôle lié à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, groupes ou groupes.

détails de politique

- Type : Politique de rôles liée à un service
- Heure de création : 16 avril 2019, 16:52 UTC
- Heure modifiée : 16 avril 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les autorisations de politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques gérées et évoluez et évoluez politiques AWS gérées et évoluez d'autorisations de politiques gérées et évoluez politiques gérées](#)

AmazonWorkMailFullAccess

AmazonWorkMailFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Directory Service WorkMail, SES, EC2 et un accès en lecture aux métadonnées KMS.

Utilisation de cette stratégie

Vous pouvez AmazonWorkMailFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 21 décembre 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ds:AuthorizeApplication",
      "ds:CheckAlias",
      "ds:CreateAlias",
      "ds:CreateDirectory",
      "ds:CreateIdentityPoolDirectory",
      "ds>DeleteDirectory",
      "ds:DescribeDirectories",
      "ds:GetDirectoryLimits",
      "ds:ListAuthorizedApplications",
      "ds:UnauthorizeApplication",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2:CreateSubnet",
      "ec2:CreateTags",
      "ec2:CreateVpc",
      "ec2>DeleteSecurityGroup",
      "ec2>DeleteSubnet",
      "ec2>DeleteVpc",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "kms:DescribeKey",
      "kms:ListAliases",
      "lambda:ListFunctions",
      "route53:ChangeResourceRecordSets",
      "route53:ListHostedZones",
      "route53:ListResourceRecordSets",
      "route53:GetHostedZone",
      "route53domains:CheckDomainAvailability",
      "route53domains:ListDomains",
      "ses:*",
      "workmail:*",
      "iam:ListRoles",
      "logs:DescribeLogGroups",
      "logs:CreateLogGroup",
```

```

    "logs:PutRetentionPolicy",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "events.workmail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*workmail*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "events.workmail.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkMailMessageFlowFullAccess

AmazonWorkMailMessageFlowFullAccess est une [politiqueAWS gérée](#) qui : Accès complet aux API WorkMail Message Flow

Utilisation de cette stratégie

Vous pouvez les associer AmazonWorkMailMessageFlowFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 février 2021, 11:08 UTC
- Heure modifiée : 11 février 2021, 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkMailMessageFlowReadOnlyAccess

AmazonWorkMailMessageFlowReadOnlyAccess est une [politiqueAWS gérée](#) qui : Accès en lecture seule aux WorkMail messages de l' GetRawMessageContent API

Utilisation de cette stratégie

Vous pouvez les associer AmazonWorkMailMessageFlowReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la stratégie

- Type : politiqueAWS gérée
- Heure de création : 28 janvier 2021, 12:40 UTC
- Heure modifiée : 28 janvier 2021, 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkMailReadOnlyAccess

AmazonWorkMailReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à WorkMail et SES.

Utilisation de cette stratégie

Vous pouvez AmazonWorkMailReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 25 juillet 2019, 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkSpacesAdmin

AmazonWorkSpacesAdmin est un [AWS politique gérée](#) qui : Fournit un accès à AmazonWorkSpacesactions administratives viaAWSSDK et CLI.

Utilisation de cette politique

Vous pouvez joindreAmazonWorkSpacesAdminà vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 22 septembre 2015, 22h21 UTC
- Heure de modification :3 août 2023, 23 h 57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

Version de la politique

Version de la politique : v5(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",

```

```
    "workspaces:CreateStandbyWorkspaces",
    "workspaces>DeleteTags",
    "workspaces:DescribeTags",
    "workspaces:DescribeWorkspaceBundles",
    "workspaces:DescribeWorkspaceDirectories",
    "workspaces:DescribeWorkspaces",
    "workspaces:DescribeWorkspacesConnectionStatus",
    "workspaces:ModifyCertificateBasedAuthProperties",
    "workspaces:ModifySamlProperties",
    "workspaces:ModifyWorkspaceProperties",
    "workspaces:RebootWorkspaces",
    "workspaces:RebuildWorkspaces",
    "workspaces:RestoreWorkspace",
    "workspaces:StartWorkspaces",
    "workspaces:StopWorkspaces",
    "workspaces:TerminateWorkspaces"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess est une [politique AWS gérée](#) qui : fournit un accès administrateur pour empaqueter une application dans Amazon WorkSpaces Application Manager.

Utilisation de cette stratégie

Vous pouvez les associer AmazonWorkSpacesApplicationManagerAdminAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 avril 2015, 14:03 UTC
- Heure modifiée : 09 avril 2015, 14:03 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonWorkSpacesApplicationManagerAdminAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkspacesPCAAccess

AmazonWorkspacesPCAAccess est une [politique AWS gérée](#) qui : [Cette politique](#) gérée fournit un accès administratif complet aux ressources de l'autorité de certification privée de AWS Certificate Manager qui se trouvent dans votre Compte AWS système pour une authentification basée sur des certificats.

Utilisation de cette stratégie

Vous pouvez AmazonWorkspacesPCAAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 novembre 2022, 00:25 UTC
- Heure modifiée : 8 novembre 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ]
    }
  ],
}
```

```
"Resource" : "arn::*:acm-pca::*:*:*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/euc-private-ca" : "*"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkSpacesSelfServiceAccess

AmazonWorkSpacesSelfServiceAccess est une [politiqueAWS gérée](#) qui : Fournit un accès au service de WorkSpaces backend Amazon pour effectuer des actions Workspace Self Service

Utilisation de cette stratégie

Vous pouvez AmazonWorkSpacesSelfServiceAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 juin 2019, 19:22 UTC
- Heure modifiée : 27 juin 2019, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkSpacesServiceAccess

AmazonWorkSpacesServiceAccess est une [politique AWS gérée](#) qui : fournit au compte client un accès au AWS WorkSpaces service pour le lancement d'un espace de travail.

Utilisation de cette stratégie

Vous pouvez les associer AmazonWorkSpacesServiceAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 juin 2019, 19:19 UTC
- Heure modifiée : 18 mars 2020, 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon WorkSpaces Web et à ses dépendances via le AWS Management Console SDK et l'interface de ligne de commande.

Utilisation de cette stratégie

Vous pouvez AmazonWorkSpacesWebReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 novembre 2021, 14:20 UTC
- Heure modifiée : 2 novembre 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",

```

```
    "workspaces-web:GetTrustStore",
    "workspaces-web:GetTrustStoreCertificate",
    "workspaces-web:GetUserSettings",
    "workspaces-web:GetUserAccessLoggingSettings",
    "workspaces-web:ListBrowserSettings",
    "workspaces-web:ListIdentityProviders",
    "workspaces-web:ListNetworkSettings",
    "workspaces-web:ListPortals",
    "workspaces-web:ListTagsForResource",
    "workspaces-web:ListTrustStoreCertificates",
    "workspaces-web:ListTrustStores",
    "workspaces-web:ListUserSettings",
    "workspaces-web:ListUserAccessLoggingSettings"
  ],
  "Resource" : "arn:aws:workspaces-web:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "kinesis:ListStreams"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise l'accès Services AWS aux ressources utilisées ou gérées par Amazon WorkSpaces Web

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Informations des des de politique

- Type : Politique de rôles liée à un service
- Heure de création : 30 novembre 2021, 13:15 UTC
- Heure modifiée : 15 décembre 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations gérées et évoluez vers les autorisations gérées et évoluez vers les autorisations gérées](#)

AmazonZocaloFullAccess

AmazonZocaloFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Zocalo.

Utilisation de cette stratégie

Vous pouvez les associer AmazonZocaloFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
```

```
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmazonZocaloReadOnlyAccess

AmazonZocaloReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Zocalo

Utilisation de cette stratégie

Vous pouvez AmazonZocaloReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccess est une [politique AWS gérée](#) qui : fournit à Amplify des autorisations d'accès complètes pour déployer les ressources principales d'Amplify (Amazon AWS AppSync Cognito, Amazon S3 et autres services connexes) via le kit de développement (CDK) AWS Cloud AWS

Utilisation de cette politique

Vous pouvez vous associer `AmplifyBackendDeployFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 06 octobre 2023, 21:32 UTC
- Heure modifiée : 2 janvier 2024, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ]
    }
  ],
}
```

```
{
  "Sid" : "AmplifyMetadata",
  "Effect" : "Allow",
  "Action" : [
    "amplify:ListApps",
    "cloudformation:ListStacks",
    "ssm:DescribeParameters",
    "appsync:GetIntrospectionSchema",
    "amplify:GetBackendEnvironment"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AmplifyHotSwappableResources",
  "Effect" : "Allow",
  "Action" : [
    "appsync:GetSchemaCreationStatus",
    "appsync:StartSchemaCreation",
    "appsync:UpdateResolver",
    "appsync:ListFunctions",
    "appsync:UpdateFunction",
    "appsync:UpdateApiKey"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AmplifyHotSwappableSchemaResource",
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction",
    "lambda:UpdateFunctionCode"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:amplify-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
```

```
  },
  {
    "Sid" : "AmplifySchema",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*amplify*",
      "arn:aws:s3:::cdk-*-assets-*-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "CDKDeploy",
    "Effect" : "Allow",
    "Action" : [
      "sts:AssumeRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
      "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
      "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
      "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AmplifySSM",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParametersByPath",
      "ssm:GetParameters",
      "ssm:GetParameter"
    ],
    "Resource" : [
```

```
    "arn:aws:ssm:*:*:parameter/amplify/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AmplifyModifySSMParam",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm>DeleteParameter",
    "ssm>DeleteParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à API Gateway de gérer les AWS ressources associées pour le compte du client.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 20 octobre 2017, 17:23 UTC
- Heure modifiée : 12 juillet 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Version de la politique

Version de la politique :v9 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
```

```
    "logs:DeleteLogDelivery",
    "logs:ListLogDeliveries",
    "servicediscovery:DiscoverInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate",
    "acm:GetCertificate"
  ],
  "Resource" : "arn:aws:acm:*:*:certificate/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterfacePermission",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Owner",
        "VpcLinkId"
      ]
    }
  }
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:ModifyNetworkInterfaceAttribute",
  "ec2>DeleteNetworkInterface",
  "ec2:AssignPrivateIpAddresses",
  "ec2:CreateNetworkInterface",
  "ec2>DeleteNetworkInterfacePermission",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeNetworkInterfaceAttribute",
  "ec2:DescribeVpcs",
  "ec2:DescribeNetworkInterfacePermissions",
  "ec2:UnassignPrivateIpAddresses",
  "ec2:DescribeSubnets",
  "ec2:DescribeRouteTables",
  "ec2:DescribeSecurityGroups"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "servicediscovery:GetNamespace",
  "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
},
{
  "Effect" : "Allow",
  "Action" : "servicediscovery:GetService",
  "Resource" : "arn:aws:servicediscovery:*:*:service/*"
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : Permet AppIntegrations de gérer les AppFlow ressources et de publier des données CloudWatch métriques en votre nom.

Utilisation des des des des des des

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, des groupes ou des rôles attachés à d'un rôle d'utilisateur, un groupe ou un rôle

Détails des des des des

- Type : Politique de rôles liée à un service
- Heure de création : 30 septembre 2022, 19:42 UTC
- Heure modifiée : 30 septembre 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations de la des autorisations de la des autorisations de la des autorisations de la des Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de de de de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des AWS moindre privilège moindre privilège moindre privilège moindre privilège moindre privilège moindre privilège moindre privilège moindre privilège moindre privilège](#)

ApplicationAutoScalingForAmazonAppStreamAccess

ApplicationAutoScalingForAmazonAppStreamAccess est une [politique AWS gérée](#) qui :
Politique visant à activer l'autodimensionnement des applications pour Amazon AppStream

Utilisation de cette stratégie

Vous pouvez les associer ApplicationAutoScalingForAmazonAppStreamAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2017, 21:39 UTC
- Heure modifiée : 6 février 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy est une [politique AWS gérée](#) qui : Permet l'accès à la fonctionnalité d'exportation continue d'Application Discovery Service Services AWS et aux ressources utilisées ou gérées par cette dernière

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 9 août 2018, 20:22 UTC
- Heure modifiée : 13 août 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
```

```

    "firehose:DescribeDeliveryStream",
    "logs:CreateLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "firehose>DeleteDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch",
    "firehose:UpdateDestination"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
},
{
  "Action" : [
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:PutBucketLogging",
    "s3:PutEncryptionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
},
{
  "Action" : [
    "s3:GetObject"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
},
{
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutRetentionPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
},
{

```

```
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "firehose.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy est une [politiqueAWS gérée](#) qui : Permet auAWS AppRunner réseau de gérer lesAWS ressources connexes en votre nom.

Utilisation de de de de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher de cette politique à vos utilisateurs, les utilisateurs, les groupes ou les rôles.

Utilisation des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 janvier 2022, 21:02 UTC
- Heure modifiée : 12 janvier 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit des autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
  ],
  {
```

```
"Effect" : "Allow",
"Action" : "ec2:CreateNetworkInterface",
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AWSAppRunnerManaged"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "StringLike" : {
      "aws:RequestTag/AWSAppRunnerManaged" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2>DeleteNetworkInterface",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
    }
  }
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS gestion et évoluez vers des autorisations de moindre privilège des autorisations de moindre privilège.](#)

AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy est une [politique AWS gérée](#) qui : Permet AWS AppRunner de gérer les AWS ressources connexes en votre nom.

Utilisation cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 14 mai 2021, 19:15 UTC
- Heure modifiée : 14 mai 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingConsoleFullAccess

AutoScalingConsoleFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Auto Scaling via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAutoScalingConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 12 janvier 2017, 19:43 UTC
- Heure modifiée : 6 février 2018, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:Describe*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:ListSubscriptions",
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:ListRoles",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    }
  }
}
```

```
    }  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec des stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingConsoleReadOnlyAccess

AutoScalingConsoleReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Auto Scaling via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAutoScalingConsoleReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 12 janvier 2017, 19:48 UTC
- Heure modifiée : 12 janvier 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingFullAccess

AutoScalingFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Auto Scaling.

Utilisation de cette stratégie

Vous pouvez AutoScalingFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 12 janvier 2017, 19:31 UTC
- Heure modifiée : 6 février 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricAlarm",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstances",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribePlacementGroups",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSpotInstanceRequests",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcClassicLink"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    }
  }
]
```



```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingNotificationAccessRole

AutoScalingNotificationAccessRole est une [politiqueAWS gérée](#) qui : Stratégie par défaut pour le rôle de service AutoScaling Notification Access.

Utilisation de cette stratégie

Vous pouvez les associer AutoScalingNotificationAccessRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingReadOnlyAccess

AutoScalingReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Auto Scaling.

Utilisation de cette stratégie

Vous pouvez AutoScalingReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 12 janvier 2017, 19:39 UTC
- Heure modifiée : 12 janvier 2017, 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AutoScalingServiceRolePolicy

AutoScalingServiceRolePolicy est une [politique AWS gérée](#) qui : autorise l'accès Services AWS aux ressources utilisées ou gérées par Auto Scaling

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 08 janvier 2018, 23h10 UTC
- Heure modifiée : 29 février 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateTags",
```

```

    "ec2:DeleteTags",
    "ec2:Describe*",
    "ec2:DetachClassicLinkVpc",
    "ec2:GetInstanceTypesFromInstanceRequirements",
    "ec2:GetSecurityGroupsForVpc",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2InstanceProfileManagement",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com*"
    }
  }
},
{
  "Sid" : "EC2SpotManagement",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "spot.amazonaws.com"
    }
  }
},
{
  "Sid" : "ELBManagement",
  "Effect" : "Allow",
  "Action" : [

```

```
    "elasticloadbalancing:Register*",
    "elasticloadbalancing:Deregister*",
    "elasticloadbalancing:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWManagement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSManagement",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EventBridgeRuleManagement",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events>DeleteRule",
    "events:DescribeRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "SystemsManagerParameterManagement",
```

```
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VpcLatticeManagement",
    "Effect" : "Allow",
    "Action" : [
      "vpc-lattice:DeregisterTargets",
      "vpc-lattice:GetTargetGroup",
      "vpc-lattice:ListTargets",
      "vpc-lattice:ListTargetGroups",
      "vpc-lattice:RegisterTargets"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWS_ConfigRole

AWS_ConfigRole est une [politique AWS gérée qui : Politique](#) par défaut pour le rôle de service AWS Config. Fournit les autorisations requises pour que AWS Config puisse suivre les modifications apportées à vos AWS ressources.

Utilisation de cette politique

Vous pouvez vous associer AWS_ConfigRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 15 septembre 2020, 20h30 UTC

- Heure modifiée : 22 février 2024, 21:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

Version de la politique

Version de la politique : v30 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
```



```
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"apigateway:GET",
"app-integrations:GetEventIntegration",
"app-integrations:ListEventIntegrationAssociations",
"app-integrations:ListEventIntegrations",
"appconfig:GetApplication",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetExtensionAssociation",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeFlow",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"appmesh:DescribeGatewayRoute",
"appmesh:DescribeMesh",
"appmesh:DescribeRoute",
"appmesh:DescribeVirtualGateway",
"appmesh:DescribeVirtualNode",
"appmesh:DescribeVirtualRouter",
"appmesh:DescribeVirtualService",
"appmesh:ListGatewayRoutes",
"appmesh:ListMeshes",
"appmesh:ListRoutes",
"appmesh:ListTagsForResource",
"appmesh:ListVirtualGateways",
"appmesh:ListVirtualNodes",
"appmesh:ListVirtualRouters",
"appmesh:ListVirtualServices",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
```

```
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"appstream:DescribeApplications",
"appstream:DescribeDirectoryConfigs",
"appstream:DescribeFleets",
"appstream:DescribeStacks",
"appstream:ListTagsForResource",
"appsync:GetApiCache",
"appsync:GetGraphQLApi",
"appsync:ListGraphQLApis",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"APS:DescribeRuleGroupsNamespace",
"APS:DescribeWorkspace",
"aps:ListRuleGroupsNamespaces",
"aps:ListTagsForResource",
"APS:ListWorkspaces",
"athena:GetDataCatalog",
"athena:GetPreparedStatement",
"athena:GetWorkGroup",
"athena:ListDataCatalogs",
"athena:ListPreparedStatements",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:ListAssessments",
"autoscaling-plans:DescribeScalingPlanResources",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeLaunchConfigurations",
"autoscaling:DescribeLifecycleHooks",
"autoscaling:DescribePolicies",
"autoscaling:DescribeScheduledActions",
"autoscaling:DescribeTags",
"autoscaling:DescribeWarmPool",
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:DescribeBackupVault",
"backup:DescribeFramework",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
```

```
"backup:DescribeReportPlan",
"backup:GetBackupPlan",
"backup:GetBackupSelection",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch:ListTagsForResource",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListTagsForResource",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionsForBudget",
"budgets:ViewBudget",
"cassandra:Select",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
```

```
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListEventDataStores",
"cloudtrail:ListTags",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:DescribeAnomalyDetectors",
"cloudwatch:GetDashboard",
"cloudwatch:GetMetricStream",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"cloudwatch:ListTagsForResource",
"codeartifact:DescribeRepository",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListTagsForResource",
"codebuild:BatchGetReportGroups",
"codebuild:ListReportGroups",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:ListRepositories",
"codecommit:ListTagsForResource",
"codedeploy:GetDeploymentConfig",
"codeguru-profiler:DescribeProfilingGroup",
"codeguru-profiler:GetNotificationConfiguration",
"codeguru-profiler:GetPolicy",
"codeguru-profiler:ListProfilingGroups",
"codeguru-reviewer:DescribeRepositoryAssociation",
"codeguru-reviewer:ListRepositoryAssociations",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"cognito-identity:DescribeIdentityPool",
```

```
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetPrincipalTagAttributeMap",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:DescribeIdentityProvider",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:GetGroup",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config:Select*",
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
```

```
"connect:ListTagsForResource",
"connect:ListTaskTemplates",
"connect:ListUsers",
"connect:SearchAvailablePhoneNumbers",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"datasync:DescribeAgent",
"datasync:DescribeLocationEfs",
"datasync:DescribeLocationFsxLustre",
"datasync:DescribeLocationFsxWindows",
"datasync:DescribeLocationHdfs",
"datasync:DescribeLocationNfs",
"datasync:DescribeLocationObjectStorage",
"datasync:DescribeLocationS3",
"datasync:DescribeLocationSmb",
"datasync:DescribeTask",
"datasync:ListAgents",
"datasync:ListLocations",
"datasync:ListTagsForResource",
"datasync:ListTasks",
"dax:DescribeClusters",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"detective:ListGraphs",
"detective:ListTagsForResource",
"devicefarm:GetInstanceProfile",
"devicefarm:GetNetworkProfile",
"devicefarm:GetProject",
"devicefarm:GetTestGridProject",
"devicefarm:ListInstanceProfiles",
"devicefarm:ListNetworkProfiles",
```

```
"devicefarm:ListProjects",
"devicefarm:ListTagsForResource",
"devicefarm:ListTestGridProjects",
"devops-guru:GetResourceCollection",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"dms:DescribeReplicationInstances",
"dms:DescribeReplicationSubnetGroups",
"dms:DescribeReplicationTaskAssessmentRuns",
"dms:DescribeReplicationTasks",
"dms:ListTagsForResource",
"ds:DescribeDirectories",
"ds:DescribeDomainControllers",
"ds:DescribeEventTopics",
"ds:ListLogSubscriptions",
"ds:ListTagsForResource",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeDhcpOptions",
"ec2:DescribeFleets",
"ec2:DescribeNetworkAcls",
"ec2:DescribePlacementGroups",
"ec2:DescribeRouteTables",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeTags",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
```

```
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitionFamilies",
"ecs:ListTaskDefinitions",
"eks:DescribeAddon",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeIdentityProviderConfig",
"eks:DescribeNodegroup",
"eks:ListAddons",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListIdentityProviderConfigs",
"eks:ListNodegroups",
"eks:ListTagsForResource",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheParameters",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
```



```
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticache:ListTagsForResource",
"elasticbeanstalk:DescribeConfigurationSettings",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"es:DescribeDomain",
"es:DescribeDomains",
```

```
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:GetCompatibleElasticsearchVersions",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListTags",
"events:DescribeApiDestination",
"events:DescribeArchive",
"events:DescribeConnection",
"events:DescribeEndpoint",
"events:DescribeEventBus",
"events:DescribeRule",
"events:ListApiDestinations",
"events:ListArchives",
"events:ListConnections",
"events:ListEndpoints",
"events:ListEventBuses",
"events:ListRules",
"events:ListTagsForResource",
"events:ListTargetsByRule",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"finespace:GetEnvironment",
"finespace:ListEnvironments",
"firehose:DescribeDeliveryStream",
"firehose:ListDeliveryStreams",
"firehose:ListTagsForDeliveryStream",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:ListPolicies",
"fms:ListTagsForResource",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"forecast:ListTagsForResource",
"frauddetector:GetDetectors",
```

```
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetLabels",
"frauddetector:GetModels",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListTagsForResource",
"fsx:DescribeBackups",
"fsx:DescribeDataRepositoryAssociations",
"fsx:DescribeFileSystems",
"fsx:DescribeSnapshots",
"fsx:DescribeStorageVirtualMachines",
"fsx:DescribeVolumes",
"fsx:ListTagsForResource",
"gamelift:DescribeAlias",
"gamelift:DescribeBuild",
"gamelift:DescribeFleetAttributes",
"gamelift:DescribeFleetCapacity",
"gamelift:DescribeFleetLocationAttributes",
"gamelift:DescribeFleetLocationCapacity",
"gamelift:DescribeFleetPortSettings",
"gamelift:DescribeGameServerGroup",
"gamelift:DescribeGameSessionQueues",
"gamelift:DescribeMatchmakingConfigurations",
"gamelift:DescribeMatchmakingRuleSets",
"gamelift:DescribeRuntimeConfiguration",
"gamelift:DescribeScript",
"gamelift:DescribeVpcPeeringAuthorizations",
"gamelift:DescribeVpcPeeringConnections",
"gamelift:ListAliases",
"gamelift:ListBuilds",
"gamelift:ListFleets",
"gamelift:ListGameServerGroups",
"gamelift:ListScripts",
"gamelift:ListTagsForResource",
"geo:DescribeGeofenceCollection",
"geo:DescribeMap",
"geo:DescribePlaceIndex",
"geo:DescribeRouteCalculator",
"geo:DescribeTracker",
"geo:ListGeofenceCollections",
```

```
"geo:ListMaps",
"geo:ListPlaceIndexes",
"geo:ListRouteCalculators",
"geo:ListTrackerConsumers",
"geo:ListTrackers",
"globalaccelerator:DescribeAccelerator",
"globalaccelerator:DescribeEndpointGroup",
"globalaccelerator:DescribeListener",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"globalaccelerator:ListTagsForResource",
"glue:BatchGetDevEndpoints",
"glue:BatchGetJobs",
"glue:BatchGetWorkflows",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobs",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTags",
"glue:GetWorkflow",
"glue:ListCrawlers",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListWorkflows",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
```

```
"greengrass:GetComponent",
"greengrass:ListComponents",
"greengrass:ListComponentVersions",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMissionProfile",
"groundstation:ListConfigs",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListMissionProfiles",
"groundstation:ListTagsForResource",
"guardduty:DescribePublishingDestination",
"guardduty:GetAdministratorAccount",
"guardduty:GetDetector",
"guardduty:GetFilter",
"guardduty:GetFindings",
"guardduty:GetIPSet",
"guardduty:GetMasterAccount",
"guardduty:GetMemberDetectors",
"guardduty:GetMembers",
"guardduty:GetThreatIntelSet",
"guardduty:ListDetectors",
"guardduty:ListFilters",
"guardduty:ListFindings",
"guardduty:ListIPSets",
"guardduty:ListMembers",
"guardduty:ListOrganizationAdminAccounts",
"guardduty:ListPublishingDestinations",
"guardduty:ListTagsForResource",
"guardduty:ListThreatIntelSets",
"healthlake:DescribeFHIRDatastore",
"healthlake:ListFHIRDatastores",
"healthlake:ListTagsForResource",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetInstanceProfile",
"iam:GetOpenIDConnectProvider",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
```

```
"iam:GetRolePolicy",
"iam:GetSAMLProvider",
"iam:GetServerCertificate",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:ListAccessKeys",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedRolePolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListGroupsForUser",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListInstanceProfileTags",
"iam:ListMFADevices",
"iam:ListMFADeviceTags",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicyVersions",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:GetComponent",
"imagebuilder:GetContainerRecipe",
"imagebuilder:GetDistributionConfiguration",
"imagebuilder:GetImage",
"imagebuilder:GetImagePipeline",
"imagebuilder:GetImageRecipe",
"imagebuilder:GetInfrastructureConfiguration",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponent",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"inspector2:BatchGetAccountStatus",
```

```
"inspector2:GetDelegatedAdminAccount",
"inspector2:ListFilters",
"inspector2:ListMembers",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeCustomMetric",
"iot:DescribeDimension",
"iot:DescribeDomainConfiguration",
"iot:DescribeFleetMetric",
"iot:DescribeJobTemplate",
"iot:DescribeMitigationAction",
"iot:DescribeProvisioningTemplate",
"iot:DescribeRoleAlias",
"iot:DescribeScheduledAudit",
"iot:DescribeSecurityProfile",
"iot:GetPolicy",
"iot:GetTopicRule",
"iot:GetTopicRuleDestination",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCustomMetrics",
"iot:ListDimensions",
"iot:ListDomainConfigurations",
"iot:ListFleetMetrics",
"iot:ListJobTemplates",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListScheduledAudits",
"iot:ListSecurityProfiles",
"iot:ListSecurityProfilesForTarget",
"iot:ListTagsForResource",
"iot:ListTargetsForSecurityProfile",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:ValidateSecurityProfileBehaviors",
"iotanalytics:DescribeChannel",
"iotanalytics:DescribeDataset",
"iotanalytics:DescribeDatastore",
```

```
"iotanalytics:DescribePipeline",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotanalytics:ListTagsForResource",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"iotsitewise:DescribeAccessPolicy",
"iotsitewise:DescribeAsset",
"iotsitewise:DescribeAssetModel",
"iotsitewise:DescribeDashboard",
"iotsitewise:DescribeGateway",
"iotsitewise:DescribePortal",
"iotsitewise:DescribeProject",
"iotsitewise:ListAccessPolicies",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListDashboards",
"iotsitewise:ListGateways",
"iotsitewise:ListPortals",
"iotsitewise:ListProjectAssets",
"iotsitewise:ListProjects",
"iotsitewise:ListTagsForResource",
"iottwinmaker:GetComponentType",
"iottwinmaker:GetEntity",
"iottwinmaker:GetScene",
"iottwinmaker:GetSyncJob",
"iottwinmaker:GetWorkspace",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListSyncJobs",
"iottwinmaker:ListTagsForResource",
"iottwinmaker:ListWorkspaces",
"iotwireless:GetFuotaTask",
"iotwireless:GetMulticastGroup",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
```



```
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamKey",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreamKeys",
"ivs:ListTagsForResource",
"kafka:DescribeCluster",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:DescribeVpcConnection",
"kafka:GetClusterPolicy",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurations",
"kafka:ListScramSecrets",
"kafka:ListTagsForResource",
"kafka:ListVpcConnections",
"kafkaconnect:DescribeConnector",
"kafkaconnect:ListConnectors",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kendra:ListTagsForResource",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
```

```
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListAliases",
"kms:ListKeys",
"kms:ListResourceTags",
"lakeformation:DescribeResource",
"lakeformation:GetDataLakeSettings",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lambda:GetAlias",
"lambda:GetCodeSigningConfig",
"lambda:GetFunction",
"lambda:GetFunctionCodeSigningConfig",
"lambda:GetLayerVersion",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lambda:ListTags",
"lambda:ListVersionsByFunction",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotVersion",
"lex:DescribeResourcePolicy",
"lex:ListBotAliases",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
"lex:ListTagsForResource",
"license-manager:GetGrant",
"license-manager:GetLicense",
"license-manager:ListDistributedGrants",
"license-manager:ListLicenses",
"license-manager:ListReceivedGrants",
"lightsail:GetAlarms",
"lightsail:GetBuckets",
"lightsail:GetCertificates",
"lightsail:GetContainerServices",
```

```
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDistributions",
"lightsail:GetInstance",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:GetDataProtectionPolicy",
"logs:GetLogDelivery",
"logs:ListLogDeliveries",
"logs:ListTagsLogGroup",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:DescribeAlert",
"lookoutmetrics:DescribeAnomalyDetector",
"lookoutmetrics:ListAlerts",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutmetrics:ListMetricSets",
"lookoutmetrics:ListTagsForResource",
"lookoutvision:DescribeProject",
"lookoutvision:ListProjects",
"m2:GetEnvironment",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetClassificationExportConfiguration",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetMacieSession",
"macie2:ListCustomDataIdentifiers",
"macie2:ListTagsForResource",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
```

```
"managedblockchain:GetNode",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNodes",
"mediaconnect:DescribeFlow",
"mediaconnect:ListFlows",
"mediaconnect:ListTagsForResource",
"mediapackage-vod:DescribePackagingConfiguration",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mediapackage-vod:ListTagsForResource",
"mediatailor:GetPlaybackConfiguration",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeAcls",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:DescribeSubnetGroups",
"memorydb:DescribeUsers",
"memorydb:ListTags",
"mobiletargeting:GetApp",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetApps",
"mobiletargeting:GetCampaign",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetEmailChannel",
"mobiletargeting:GetEmailTemplate",
"mobiletargeting:GetEventStream",
"mobiletargeting:GetInAppTemplate",
"mobiletargeting:GetSegment",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTagsForResource",
"mobiletargeting:ListTemplates",
"mq:DescribeBroker",
"mq:ListBrokers",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectPeer",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
```

```
"networkmanager:GetSites",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:ListConnectPeers",
"networkmanager:ListTagsForResource",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetStreamingImage",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStudioComponents",
"nimble:ListStudios",
"opsworks:DescribeInstances",
"opsworks:DescribeLayers",
"opsworks:DescribeTimeBasedAutoScaling",
"opsworks:DescribeVolumes",
"opsworks:ListTags",
"organizations:DescribeAccount",
"organizations:DescribeEffectivePolicy",
"organizations:DescribeOrganization",
"organizations:DescribeOrganizationalUnit",
"organizations:DescribePolicy",
"organizations:DescribeResourcePolicy",
"organizations:ListAccounts",
"organizations:ListAccountsForParent",
"organizations:ListDelegatedAdministrators",
"organizations:ListOrganizationalUnitsForParent",
"organizations:ListParents",
"organizations:ListPolicies",
"organizations:ListPoliciesForTarget",
"organizations:ListRoots",
"organizations:ListTagsForResource",
"organizations:ListTargetsForPolicy",
"panorama:DescribeApplicationInstance",
"panorama:DescribeApplicationInstanceDetails",
"panorama:DescribePackage",
"panorama:DescribePackageVersion",
"panorama:ListApplicationInstances",
"panorama:ListNodes",
"panorama:ListPackages",
"personalize:DescribeDataset",
"personalize:DescribeDatasetGroup",
"personalize:DescribeSchema",
```

```
"personalize:DescribeSolution",
"personalize:ListDatasetGroups",
"personalize:ListDatasetImportJobs",
"personalize:ListDatasets",
"personalize:ListSchemas",
"personalize:ListSolutions",
"personalize:ListTagsForResource",
"profile:GetDomain",
"profile:GetIntegration",
"profile:GetProfileObjectType",
"profile:ListDomains",
"profile:ListIntegrations",
"profile:ListProfileObjectTypes",
"profile:ListTagsForResource",
"quicksight:DescribeAccountSubscription",
"quicksight:DescribeAnalysis",
"quicksight:DescribeAnalysisPermissions",
"quicksight:DescribeDashboard",
"quicksight:DescribeDashboardPermissions",
"quicksight:DescribeDataSet",
"quicksight:DescribeDataSetPermissions",
"quicksight:DescribeDataSetRefreshProperties",
"quicksight:DescribeDataSource",
"quicksight:DescribeDataSourcePermissions",
"quicksight:DescribeTemplate",
"quicksight:DescribeTemplatePermissions",
"quicksight:DescribeTheme",
"quicksight:DescribeThemePermissions",
"quicksight:ListAnalyses",
"quicksight:ListDashboards",
"quicksight:ListDataSets",
"quicksight:ListDataSources",
"quicksight:ListTagsForResource",
"quicksight:ListTemplates",
"quicksight:ListThemes",
"ram:GetPermission",
"ram:GetResourceShareAssociations",
"ram:GetResourceShares",
"ram:ListPermissionAssociations",
"ram:ListPermissions",
"ram:ListPermissionVersions",
"ram:ListResources",
"ram:ListResourceSharePermissions",
"rds:DescribeDBClusterParameterGroups",
```

```
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:ListTagsForResource",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEndpointAccess",
"redshift:DescribeEndpointAuthorization",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeLoggingStatus",
"redshift:DescribeScheduledActions",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"rekognition:DescribeStreamProcessor",
"rekognition:ListStreamProcessors",
"rekognition:ListTagsForResource",
"resiliencehub:DescribeApp",
```

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

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSAccountActivityAccess

AWSAccountActivityAccess est une [politiqueAWS gérée](#) qui : Autorise les utilisateurs à accéder à la page d'activité du compte.

Utilisation de la stratégie

Vous pouvez AWSAccountActivityAccess les associer à vos utilisateurs, groupes et rôles.

Détails des la politique

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 07 mars 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "account:GetAccountInformation",
      "account:GetAlternateContact",
      "account:GetChallengeQuestions",
      "account:GetContactInformation",
      "account:GetRegionOptStatus",
      "account:ListRegions",
      "billing:GetIAMAccessPreference",
      "billing:GetSellerOfRecord",
      "payments:ListPaymentPreferences"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-portal:ViewBilling"
    ],
    "Resource" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAccountManagementFullAccess

AWSAccountManagementFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à la gestion des AWS comptes.

Utilisation de la stratégie

Vous pouvez les associer AWSAccountManagementFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des la stratégie

- Type : politiqueAWS gérée
- Heure de création : 30 septembre 2021, 23h20 UTC
- Heure modifiée : 30 septembre 2021, 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à la gestion desAWS comptes

Utilisation de cette stratégie

Vous pouvez les associerAWSAccountManagementReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 septembre 2021, 23:29 UTC
- Heure modifiée : 30 septembre 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAccountUsageReportAccess

AWSAccountUsageReportAccess est une [politiqueAWS gérée](#) qui : Autorise les utilisateurs à accéder à la page du rapport d'utilisation du compte.

Utilisation de cette stratégie

Vous pouvezAWSAccountUsageReportAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-portal:ViewUsage"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAgentlessDiscoveryService

AWSAgentlessDiscoveryServiceest une [politiqueAWS gérée](#) qui : permet au connecteur Discovery Agentless de s'enregistrer auprès d'AWSApplication Discovery Service.

Utilisation de cette stratégie

Vous pouvezAWSAgentlessDiscoveryService les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 2 août 2016, 01:35 UTC
- Heure modifiée : 24 février 2020, 23:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
    "s3:PutObjectAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
},
{
  "Sid" : "Discovery",
  "Effect" : "Allow",
  "Action" : [
    "Discovery:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "arsenal",
  "Effect" : "Allow",
  "Action" : [
    "arsenal:RegisterOnPremisesAgent"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "mgh:GetHomeRegion"
  ],
  "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppFabricFullAccess

AWSAppFabricFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet au AWS AppFabric service et un accès en lecture seule aux services dépendants tels que S3, Kinesis, KMS.

Utilisation de cette politique

Vous pouvez l'associer AWSAppFabricFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 19:51 UTC
- Heure modifiée : 27 juin 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "KMSListAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3ReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "FirehoseReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowUseOfServiceLinkedRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "appfabric.amazonaws.com"
    }
  },
  "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
}
]
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSAppFabricReadOnlyAccess

AWSAppFabricReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à AWS AppFabric

Utilisation de cette politique

Vous pouvez l'associer AWSAppFabricReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 19:52 UTC
- Heure modifiée : 27 juin 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "appfabric:GetAppAuthorization",
      "appfabric:GetAppBundle",
      "appfabric:GetIngestion",
      "appfabric:GetIngestionDestination",
      "appfabric:ListAppAuthorizations",
      "appfabric:ListAppBundles",
      "appfabric:ListIngestionDestinations",
      "appfabric:ListIngestions",
      "appfabric:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un AppFabric accès aux AWS ressources en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service

- Heure de création : 26 juin 2023, 21:07 UTC
- Heure modifiée : 26 juin 2023, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
```

```
    "s3:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "FirehosePutRecord",
  "Effect" : "Allow",
  "Action" : [
    "firehose:PutRecordBatch"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "aws:ResourceTag/AWSAppFabricManaged" : "true"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy est une [politique AWS gérée](#) qui :
Politique accordant des autorisations à Application Auto Scaling pour accéder à AppStream et CloudWatch.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 20 octobre 2017, 19:04 UTC
- Heure modifiée : 20 octobre 2017, 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez les autorisations de moindre privilège](#)

AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy est une [politique AWS gérée](#) qui :
Politique accordant des autorisations à Application Auto Scaling pour accéder à Cassandra et CloudWatch.

Utilisation des stratégies

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 18 mars 2020, 22:49 UTC
- Heure modifiée : 18 mars 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
      ]
    }
  ]
}
```

```
    "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cassandra:Alter",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

AWSApplicationAutoscalingComprehendEndpointPolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à Application Auto Scaling pour accéder à Comprehend et CloudWatch.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails

- Type : Politique de rôles liée à un service
- Heure de création : 14 novembre 2019, 18:39 UTC
- Heure modifiée : 14 novembre 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politique AWS gérée et évoluez vers les autorisations](#)

AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy est une [politique AWS gérée](#) qui : [Politique](#) accordant des autorisations à Application Auto Scaling pour accéder à ApiGateway et CloudWatch pour une mise à l'échelle personnalisée des ressources

Utilisation politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 juin 2018, 23:22 UTC
- Heure modifiée : 4 juin 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy est une [politiqueAWS gérée](#) qui :
Politique accordant des autorisations à Application Auto Scaling pour accéder à DynamoDB et CloudWatch.

Utilisation de cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique politique politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 20 octobre 2017, 21:34 UTC
- Heure modifiée : 20 octobre 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de politique est la version qui définit les autorisations pour la stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à Application Auto Scaling pour accéder à EC2 Spot Fleet et CloudWatch.

Utilisation de cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

détails politiques politiques politiques politiques

- Type : Politique de rôles liée à un service

- Heure de création : 25 octobre 2017, 18:23 UTC
- Heure modifiée : 25 octobre 2017, 18:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de politique est la version qui définit les autorisations pour la politique par défaut de politique est la version qui définit les autorisations pour politiques par défaut de stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON document de

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec politiques AWS gérées gérées gérées gérées et évoluez vers les autorisations de moindre privilège de moindre privilège de moindre privilège de moindre privilège](#)

AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à Application Auto Scaling pour accéder à EC2 Container Service et CloudWatch.

Utilisation de cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 25 octobre 2017, 23:53 UTC
- Heure modifiée : 25 octobre 2017, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations de politique de politique qui définit les autorisations des politiques qui définit les autorisations de politique de politique qui Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON politique de

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

```
"Effect" : "Allow",
"Action" : [
  "ecs:DescribeServices",
  "ecs:UpdateService",
  "cloudwatch:PutMetricAlarm",
  "cloudwatch:DescribeAlarms",
  "cloudwatch>DeleteAlarms"
],
"Resource" : [
  "*"
]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Utilisation des stratégies de moindre privilège deAWS moindre privilège de moindre privilège des autorisations de moindre privilège de moindre privilège des autorisations de moindre privilège](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy est une [politiqueAWS gérée](#) qui :
Politique accordant des autorisations à Application Auto Scaling pour accéder à Amazon ElastiCache et Amazon CloudWatch.

Utilisation de cette politique de politique Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des stratégies de politique de politique de politique de politique de politique de

Utilisation des politiques politiques politiques

- Type : Politique de rôles liée à un service
- Utilisation des stratégies de création des stratégies de création des stratégies de création des stratégies de création des stratégies de création d'un
- Heure modifiée : 17 août 2021, 23:41 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut des politiques politiques politiques politiques politiques politiques politiques politiques politiques politiques de politique de politique de politique de politique de politique de politique de politique de politique de stratégie Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON des politiques

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


Document de stratégie de stratégie de stratégie

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy est une [politiqueAWS gérée qui : Politique](#) accordant des autorisations à Application Auto Scaling pour accéder au Managed Streaming for Apache Kafka et CloudWatch.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails de politique

- Type : Politique de rôles liée à un service
- Heure de création : 24 août 2020, 18:36 UTC

- Heure modifiée : 24 août 2020, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy est une [politique AWS gérée](#) qui : Politique accordant des autorisations à Application Auto Scaling pour accéder à Lambda et CloudWatch.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, vos groupes ou vos rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 octobre 2019, 20:04 UTC
- Heure modifiée : 21 octobre 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",

```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy est une [politiqueAWS gérée](#) qui :
Politique accordant des autorisations à Application Auto Scaling pour accéder à Amazon Neptune et Amazon CloudWatch.

Using this policy

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à des groupes ou

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 2 septembre 2021, 21:14 UTC
- Heure modifiée : 2 septembre 2021, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La politique est Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

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*"
    ]
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [DémarrerAWS](#)

AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à Application Auto Scaling pour accéder à RDS et CloudWatch.

Utilisation des stratégies IAM

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à un service qui permet à un service qui permet à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 octobre 2017, 17:46 UTC
- Heure modifiée : 7 août 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON Document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

AWSApplicationAutoscalingSageMakerEndpointPolicy est une [politique AWS gérée](#) qui : Politique accordant des autorisations à Application Auto Scaling pour accéder à SageMaker et CloudWatch.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 6 février 2018, 19:58 UTC
- Heure modifiée : 13 novembre 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess est une [politique AWS gérée](#) qui : permet à l'agent Discovery de s'enregistrer auprès d'AWSApplication Discovery Service.

Utilisation de cette stratégie

Vous pouvez AWSApplicationDiscoveryAgentAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 mai 2016, 21:38 UTC
- Heure modifiée : 24 février 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess est une [politiqueAWS gérée](#) qui :
Permet aux collecteurs sans agent Application Discovery Service de se mettre à jour auto, de s'enregistrer et de communiquer avec Application Discovery Service

Utilisation de cette stratégie

Vous pouvezAWSApplicationDiscoveryAgentlessCollectorAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 16 août 2022, 21:00 UTC
- Heure modifiée : 16 août 2022, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationDiscoveryAgentlessCollectorAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet pour afficher et étiqueter les éléments de configuration gérés par le AWS Application Discovery Service

Utilisation de cette stratégie

Vous pouvez AWSApplicationDiscoveryServiceFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 mai 2016, 21h30 UTC
- Heure modifiée : 19 juin 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
    },
  ]
}
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
    continuousexport.discovery.amazonaws.com/
    AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "migrationhub.amazonaws.com",
          "dmsintegration.migrationhub.amazonaws.com",
          "smsintegration.migrationhub.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationAgentInstallationPolicy

AWSApplicationMigrationAgentInstallationPolicy est une [politique AWS gérée](#) qui : Cette politique permet d'installer l'agent de AWS réplication, qui est utilisé avec AWS Application Migration Service (MGN) pour migrer des serveurs externes vers AWS. Attachez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation de l'agent de AWS réplication.

Utilisation de cette stratégie

Vous pouvez les associer `AWSApplicationMigrationAgentInstallationPolicy` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 19 juin 2022, 07:51 UTC
- Heure modifiée : 20 septembre 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
```



```
    "Effect" : "Allow",
    "Action" : [
      "mgn:IssueClientCertificateForMgn"
    ],
    "Resource" : "arn:aws:mgn:*:*:source-server/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "mgn:TagResource",
    "Resource" : "arn:aws:mgn:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "mgn:CreateAction" : "RegisterAgentForMgn"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationAgentPolicy

AWSApplicationMigrationAgentPolicy est une [politique AWS gérée](#) qui : Cette politique permet d'installer et d'utiliser l'agent de AWS réplique, qui est utilisé avec AWS Application Migration Service (MGN) pour migrer des serveurs externes vers AWS. Attachez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation de l'agent de AWS réplique.

Utilisation de cette stratégie

Vous pouvez AWSApplicationMigrationAgentPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 avril 2021, 07:00 UTC
- Heure modifiée : 20 septembre 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",

```

```
    "mgn:GetAgentRuntimeConfigurationForMgn",
    "mgn:UpdateAgentBacklogForMgn",
    "mgn:GetAgentReplicationInfoForMgn"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "mgn:TagResource",
  "Resource" : "arn:aws:mgn:*:*:source-server/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationAgentPolicy_v2

AWSApplicationMigrationAgentPolicy_v2 est une [politique AWS gérée](#) qui : Cette politique permet d'utiliser l'agent de AWS réplication, qui est utilisé avec AWS Application Migration Service (MGN) pour migrer des serveurs externes vers AWS. Nous vous déconseillons de placer cette stratégie à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvez AWSApplicationMigrationAgentPolicy_v2 les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : Politique de rôle de service
- Heure de création : 6 juin 2022, 14:14 UTC
- Heure modifiée : 6 juin 2022, 14:14 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationConversionServerPolicy

AWSApplicationMigrationConversionServerPolicy est une [politique AWS gérée](#) qui : Cette politique permet au serveur de conversion Application Migration Service (MGN), qui sont des instances EC2 lancées par Application Migration Service, de communiquer avec le service MGN. Un rôle IAM doté de cette politique est associé (en tant que profil d'instance EC2) par MGN aux serveurs de conversion MGN, qui sont automatiquement lancés et interrompus par MGN, en cas de besoin. Nous vous déconseillons de placer cette stratégie dans vos utilisateurs ou rôles IAM. Les serveurs de conversion MGN sont utilisés par Application Migration Service lorsque les utilisateurs choisissent de lancer des instances de test ou de transition à l'aide de la console, de l'interface de ligne de commande ou de l'API MGN.

Utilisation de cette stratégie

Vous pouvez AWSApplicationMigrationConversionServerPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 avril 2021, 06:48 UTC
- Heure modifiée : 7 avril 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access est une [politiqueAWS gérée](#) qui : Cette politique fournit les opérations Amazon EC2 requises pour utiliser Application Migration Service (MGN) afin de lancer les serveurs migrés en tant qu'instances EC2. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvez AWSApplicationMigrationEC2Access les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 7 avril 2021, 07:05 UTC
- Heure modifiée : 06 février 2023, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeImages",
    "ec2:DescribeVolumes"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "mgn.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "ForAnyValue:StringEquals" : {

```



```
        "aws:CalledVia" : [
            "mgn.amazonaws.com"
        ]
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "mgn.amazonaws.com"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```

    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateSecurityGroup",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
```

```
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
```

```

    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances",
          "CreateLaunchTemplate"
        ]
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2:ModifyVolume"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationFullAccess

AWSApplicationMigrationFullAccess est une [politiqueAWS gérée](#) qui : Cette politique fournit des autorisations à toutes les API publiques d'AWSApplication Migration Service (MGN), ainsi que des autorisations pour lire les informations clés KMS. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvezAWSApplicationMigrationFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 avril 2021, 06:56 UTC
- Heure modifiée : 20 avril 2023, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "mgn:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeKeyPairs",
      "ec2:DescribeTags",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribePlacementGroups",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstanceTypeOfferings",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeVolumes",
      "ec2:GetEbsEncryptionByDefault",
      "ec2:GetEbsDefaultKmsKeyId"
    ],
    "Resource" : "*"
  },
  {
```



```

    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:ListInstanceProfiles",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
      "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "drs:DescribeSourceServers"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
  },

```

```

    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      },
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListCommandInvocations"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
      "arn:aws:ssm:*:*:document/AWSMigration-*"
    ],
    "Condition" : {
      "Bool" : {

```

```

        "aws:ViaAWSService" : "true"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "drs:DisconnectSourceServer"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
        "Bool" : {
            "aws:ViaAWSService" : "true"
        },
        "Null" : {
            "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
},
{
    "Effect" : "Allow",

```

```

    "Action" : [
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
      "arn:aws:ssm:*:*:document/AWSMigration-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "mgn.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ssm:ListCommands",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationMGHAccess

AWSApplicationMigrationMGHAccess est une [politiqueAWS gérée](#) qui : Cette politique permet àAWS Application Migration Service (MGN) d'envoyer des métadonnées concernant la progression des serveurs en cours de migration à l'aide de MGN versAWS Migration Hub (MGH). MGN crée automatiquement un rôle IAM auquel cette politique est attachée et assume ce rôle. Nous vous déconseillons de placer cette stratégie dans vos utilisateurs ou rôles IAM afin de vous déconseillons de placer cette stratégie dans vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvezAWSApplicationMigrationMGHAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique de rôle de service
- Heure de création : 7 avril 2021, 07:10 UTC
- Heure modifiée : 7 avril 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM et ajout de droits](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationReadOnlyAccess

AWSApplicationMigrationReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique fournit des autorisations à toutes les API publiques en lecture seule d'Application Migration Service (MGN), ainsi qu'à certaines API en lecture seule d'autres AWS services qui sont requises pour utiliser pleinement en lecture seule la console MGN. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvez `AWSApplicationMigrationReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 avril 2021, 07:15 UTC
- Heure modifiée : 20 mars 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",

```

```
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationReplicationServerPolicy

AWSApplicationMigrationReplicationServerPolicy est une [politiqueAWS gérée](#) qui : Cette politique permet aux serveurs de réplication Application Migration Service (MGN), qui sont des instances EC2 lancées par Application Migration Service, de communiquer avec le service MGN et de créer des instantanés EBS dans votre Compte AWS. Un rôle IAM doté de cette politique

est associé (en tant que profil d'instance EC2) par Application Migration Service aux serveurs de réplication MGN qui sont automatiquement lancés et interrompus par MGN, selon les besoins. Les serveurs de réplication MGN sont utilisés pour faciliter la réplication des données depuis vos serveurs externes vers AWS, dans le cadre du processus de migration géré à l'aide de MGN. Nous vous déconseillons de placer cette stratégie à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvez associer `AWSApplicationMigrationReplicationServerPolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : Politique de rôle de service
- Heure de création : 7 avril 2021, 07:21 UTC
- Heure modifiée : 7 avril 2021, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
```

```

    "mgn:GetAgentSnapshotCreditsForMgn",
    "mgn:DescribeReplicationServerAssociationsForMgn",
    "mgn:DescribeSnapshotRequestsForMgn",
    "mgn:BatchDeleteSnapshotRequestForMgn",
    "mgn:NotifyAgentAuthenticationForMgn",
    "mgn:BatchCreateVolumeSnapshotGroupForMgn",
    "mgn:UpdateAgentReplicationProcessStateForMgn",
    "mgn:NotifyAgentReplicationProgressForMgn",
    "mgn:NotifyAgentConnectedForMgn",
    "mgn:NotifyAgentDisconnectedForMgn"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy est une [politique AWS gérée](#) qui : Cette politique permet d'installer et d'utiliser l'agent de AWS réplication, qui est utilisé par le service de migration des AWS applications (AWSMGN) pour migrer les serveurs sources qui s'exécutent sur EC2 (cross-region ou cross-AZ). Un rôle IAM conforme à cette politique doit être attaché (sous forme de profil d'instance EC2) aux instances EC2.

Utilisation de cette politique

Vous pouvez vous associer AWSApplicationMigrationServiceEc2InstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 août 2023, 13:19 UTC

- Heure modifiée : 3 janvier 2024, 14:19 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationServiceEc2InstancePolicy

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:mgn:*:*:source-server/*"
  },
  {
    "Sid" : "MgnSourceServerTagResource",
    "Effect" : "Allow",
    "Action" : "mgn:TagResource",
    "Resource" : "arn:aws:mgn:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "mgn:CreateAction" : "RegisterAgentForMgn"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy est une [politique AWS gérée](#) qui : permet au service de migration des AWS applications de créer et de gérer AWS des ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 7 avril 2021, 06:43 UTC
- Heure modifiée : 20 juin 2023, 09:12 UTC

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

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceState",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount"
  ],
  "Resource" : "arn:aws:organizations::*:account/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*"
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:DeleteSnapshot"
],
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
```



```
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
```

```
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
```

```
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "Null" : {
            "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Null" : {
            "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "Null" : {
```

```

        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam:*:*:role/service-role/AWSApplicationMigrationConversionServerRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "ec2.amazonaws.com"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringEquals" : {

```

```
    "ec2:CreateAction" : [
      "CreateLaunchTemplate",
      "CreateSecurityGroup",
      "CreateVolume",
      "CreateSnapshot",
      "RunInstances"
    ]
  }
}
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess est une [politique AWS gérée](#) qui : Cette politique donne accès aux opérations Amazon SSM requises pour utiliser Application Migration Service (MGN) afin d'exécuter des documents SSM de commande de post-migration personnalisés. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette stratégie

Vous pouvez AWSApplicationMigrationSSMAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 09:29 UTC
- Heure modifiée : 20 mars 2023, 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
        "aws:CalledVia" : [
            "mgn.amazonaws.com"
        ]
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "mgn.amazonaws.com"
            ]
        },
        "Null" : {
            "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:ListDocuments"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicyest une [politiqueAWS gérée](#) qui : Cette politique permet d'installer et d'utiliser le clientAWS vCenter, qui est utilisé avecAWS Application Migration Service (MGN) pour migrer des serveurs externes versAWS. Attachez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation deAWS vCenter Client.

Utilisation de cette stratégie

Vous pouvez les associerAWSApplicationMigrationVCenterClientPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 novembre 2021, 12:53 UTC
- Heure modifiée : 8 novembre 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn>DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess est une [politique AWS gérée](#) qui : [Politique](#) App Mesh Envoy pour accéder à la configuration de Virtual Node.

Utilisation de cette stratégie

Vous pouvez AWSAppMeshEnvoyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 juillet 2019, 21:29 UTC
- Heure modifiée : 3 juillet 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppMeshFullAccess

AWSAppMeshFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet aux APIAWS App Mesh et à la console de gestion.

Utilisation de cette stratégie

Vous pouvezAWSAppMeshFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 16 avril 2019, 17:50 UTC
- Heure modifiée : 7 janvier 2021, 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "appmesh.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStack*",
      "cloudformation:UpdateStack"
    ],
    "Resource" : "arn:aws:cloudformation::*:stack/AWSAppMesh-GettingStarted-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:ListNamespaces",
      "servicediscovery:ListServices",
      "servicediscovery:ListInstances"
    ],
    "Resource" : "*"
  }
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess est une [politiqueAWS gérée qui : Politique](#) App Mesh Preview Envoy pour accéder à la configuration de Virtual Node.

Utilisation de cette stratégie

Vous pouvezAWSAppMeshPreviewEnvoyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 5 août 2019, 23:32 UTC
- Heure modifiée : 5 août 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppMeshPreviewServiceRolePolicy

AWSAppMeshPreviewServiceRolePolicy est une [politique AWS gérée](#) qui : Active l'accès Services AWS aux ressources utilisées ou gérées par AWS App Mesh

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 juin 2019, 19:07 UTC
- Heure modifiée : 21 août 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège gérées](#)

AWSAppMeshReadOnly

AWSAppMeshReadOnly est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux API AWS App Mesh et à la console de gestion.

Utilisation de cette stratégie

Vous pouvez AWSAppMeshReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 16 avril 2019, 17:51 UTC
- Heure modifiée : 7 janvier 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStack*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:ListNamespaces",
      "servicediscovery:ListServices",
      "servicediscovery:ListInstances"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy est une [politique AWS gérée](#) qui : permet l'accès Services AWS aux ressources utilisées ou gérées par AWS AppMesh

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 03 juin 2019, 18h30 UTC
- Heure modifiée : 10 octobre 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
    }
  ]
}
```

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSAppRunnerFullAccess

`AWSAppRunnerFullAccess` est une [politique AWS gérée](#) qui : accorde des autorisations à toutes les actions d'App Runner.

Utilisation de cette stratégie

Vous pouvez `AWSAppRunnerFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 janvier 2022, 04:02 UTC
- Heure modifiée : 11 janvier 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "apprunner.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "apprunner.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AppRunnerAdminAccess",
    "Effect" : "Allow",
    "Action" : "apprunner:*",
    "Resource" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppRunnerReadOnlyAccess

AWSAppRunnerReadOnlyAccess est une [stratégie AWS gérée](#) qui : permet de répertorier et d'afficher les détails des ressources d'App Runner.

Utilisation de cette politique

Vous pouvez AWSAppRunnerReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 février 2022, 21:24 UTC
- Heure modifiée : 24 février 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppRunnerServicePolicyForECRAccess

`AWSAppRunnerServicePolicyForECRAccess` est une [politiqueAWS gérée](#) qui : Politique de serviceAWS App Runner qui accorde des autorisations de lecture aux ressources Amazon ECR du compte du client. Utilisez-le dans un rôle transmis à App Runner lors de la création ou de la mise à jour d'un service App Runner.

Utilisation de cette stratégie

Vous pouvez les associer `AWSAppRunnerServicePolicyForECRAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 mai 2021, 19:17 UTC
- Heure modifiée : 14 mai 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppSyncAdministrator

AWSAppSyncAdministrator est une [politiqueAWS gérée](#) qui : fournit un accès administratif au AppSync service, mais pas suffisant pour y accéder via la console.

Utilisation de cette stratégie

Vous pouvez les associerAWSAppSyncAdministrator à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 20 mars 2018, 21:20 UTC
- Heure modifiée : 4 novembre 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```



```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "appsync.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/AWSServiceRoleForAppSync*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess est une [politique AWS gérée](#) qui : Fournit un accès d'appel complet au AppSync service, à la fois via la console et indépendamment

Utilisation de cette stratégie

Vous pouvez AWSAppSyncInvokeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 mars 2018, 21:21 UTC

- Heure modifiée : 20 mars 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppSyncPushToCloudWatchLogs

AWSAppSyncPushToCloudWatchLogs est une [politique AWS gérée](#) qui : Permet de transférer AppSync les journaux vers le CloudWatch compte de l'utilisateur.

Utilisation de cette stratégie

Vous pouvez AWSAppSyncPushToCloudWatchLogs les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 avril 2018, 19:38 UTC
- Heure modifiée : 9 avril 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor est une [politiqueAWS gérée](#) qui : fournit un accès pour créer, mettre à jour et interroger le schéma.

Utilisation de cette stratégie

Vous pouvez les associer AWSAppSyncSchemaAuthor à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 20 mars 2018, 21:21 UTC
- Heure modifiée : 01 février 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync>DeleteResolver",
        "appsync>DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphQLApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphQLApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync>DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet l'accès auxAWS services et aux ressources utilisés ou gérés par AppSync

Utilisation cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 janvier 2020, 19:56 UTC
- Heure modifiée : 21 janvier 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingTargets",
      "xray:GetSamplingRules",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSArtifactAccountSync

AWSArtifactAccountSync est une [politiqueAWS gérée](#) qui : AutoriseAWS Artifact à accéder en lecture seule aux opérationsAWS Organizations.

Utilisation de cette stratégie

Vous pouvezAWSArtifactAccountSync les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 10 avril 2018, 23:04 UTC
- Heure modifiée : 10 avril 2018, 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSArtifactReportsReadOnlyAccess

AWSArtifactReportsReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux rapports du service AWS Artifact.

Utilisation de cette politique

Vous pouvez vous associer `AWSArtifactReportsReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 janvier 2024, 22:42 UTC
- Heure modifiée : 2 janvier 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSArtifactServiceRolePolicy

AWSArtifactServiceRolePolicy est un [AWS politique gérée](#) qui : Permet AWSArtefact permettant de recueillir des informations sur une organisation via AWSService aux organisations.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type: Politique des rôles liés aux services
- Heure de création: 21 août 2023, 20h27 UTC
- Heure modifiée :21 août 2023, 20h27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à un AWSressource, AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess est une [politique AWS gérée](#) qui : fournit un accès administratif pour activer ou désactiver AWS Audit Manager, mettre à jour les paramètres et gérer les évaluations, les contrôles et les structures

Utilisation de cette stratégie

Vous pouvez les associer AWSAuditManagerAdministratorAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 décembre 2020, 20:02 UTC
- Heure modifiée : 30 avril 2022, 00:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
    }
  ]
}
```

```

    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "organizations:ServicePrincipal" : [
          "auditmanager.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "IAMAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetUser",
      "iam:ListUsers",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMAccessCreateSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "auditmanager.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "IAMAccessManageSLR",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:UpdateRoleDescription",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
  },
  {
    "Sid" : "S3Access",

```

```
"Effect" : "Allow",
"Action" : [
  "s3:ListAllMyBuckets"
],
"Resource" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsCreateGrantAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "auditmanager.*.amazonaws.com"
    }
  }
},
{
  "Sid" : "SNSAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateEventsAccess",
  "Effect" : "Allow",
  "Action" : [
```

```
    "events:PutRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:detail-type" : "Security Hub Findings - Imported"
    },
    "ForAllValues:StringEquals" : {
      "events:source" : [
        "aws.securityhub"
      ]
    }
  }
},
{
  "Sid" : "EventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
},
{
  "Sid" : "TagAccess",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSAuditManagerServiceRolePolicy

AWSAuditManagerServiceRolePolicy est une [politique AWS gérée](#) qui : autorise l'accès Services AWS aux ressources utilisées ou gérées par AWS Audit Manager

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 08 décembre 2020, 15:12 UTC
- Heure modifiée : 6 décembre 2023, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```



```
"acm:ListCertificates",
"backup:ListRecoveryPointsByResource",
"bedrock:GetCustomModel",
"bedrock:GetFoundationModel",
"bedrock:GetModelCustomizationJob",
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:ListCustomModels",
"bedrock:ListFoundationModels",
"bedrock:ListModelCustomizationJobs",
"cloudtrail:DescribeTrails",
"cloudtrail:LookupEvents",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cognito-idp:DescribeUserPool",
"config:DescribeConfigRules",
"config:DescribeDeliveryChannels",
"config:ListDiscoveredResources",
"directconnect:DescribeDirectConnectGateways",
"directconnect:DescribeVirtualGateways",
"dynamodb:DescribeTable",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeCustomerGateways",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGateways",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeTransitGateways",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
```

```
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetEbsEncryptionByDefault",
"ecs:DescribeClusters",
"eks:DescribeAddonVersions",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeServiceUpdates",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSslPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListSecurityConfigurations",
"events:DescribeRule",
"events:ListConnections",
"events:ListEventBuses",
"events:ListEventSources",
"events:ListRules",
"firehose:ListDeliveryStreams",
"fsx:DescribeFileSystems",
"guardduty:ListDetectors",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListOpenIdConnectProviders",
"iam:ListPolicies",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSamlProviders",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"kafka:ListClusters",
"kafka:ListKafkaVersions",
"kinesis:ListStreams",
"kms:DescribeKey",
"kms:GetKeyPolicy",
```

```

    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
  ],
  "Resource" : "*",
  "Sid" : "AuditManagerAPICallAccess"
},
{
  "Sid" : "AuditManagerS3GetBucketPolicyAccess",
  "Effect" : "Allow",

```

```
"Action" : [
  "s3:GetBucketPolicy"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : [
      "${aws:PrincipalAccount}"
    ]
  }
}
},
{
  "Sid" : "CreateEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
  "Condition" : {
    "StringEquals" : {
      "events:detail-type" : "Security Hub Findings - Imported"
    },
    "Null" : {
      "events:source" : "false"
    },
    "ForAllValues:StringEquals" : {
      "events:source" : [
        "aws.securityhub"
      ]
    }
  }
},
{
  "Sid" : "EventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
```

```
    ],  
    "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"  
  }  
]  
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à AWS Auto Scaling pour prévoir périodiquement la capacité et générer des actions de dimensionnement planifiées pour les groupes Auto Scaling dans le cadre d'un plan de dimensionnement

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 août 2018, 22:46 UTC
- Heure modifiée : 23 août 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupAuditAccess

AWSBackupAuditAccess est une [politique AWS gérée](#) qui : Cette politique autorise les utilisateurs à créer des contrôles et des structures qui définissent leurs attentes en matière de ressources et d'activités de AWS Backup, et à auditer les ressources et les activités de AWS Backup par rapport à leurs contrôles et structures définis. Cette politique accorde des autorisations à AWS Config et à des services similaires pour décrire les attentes des utilisateurs et effectuer les audits. Cette politique accorde également l'autorisation de fournir des rapports d'audit à S3 et à des services similaires, et permet aux utilisateurs de rechercher et d'ouvrir leurs rapports d'audit.

Utilisation de cette stratégie

Vous pouvez les associer `AWSBackupAuditAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 août 2021, 01:02 UTC
- Heure modifiée : 10 avril 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup>DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup>DeleteReportPlan",

```

```
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "config:GetComplianceDetailsByConfigRule"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource" : "arn:aws:s3:::*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupDataTransferAccess

AWSBackupDataTransferAccess est une [politique AWS gérée](#) qui : Cette politique permet à l'agent AWS Backint d'effectuer le transfert des données de sauvegarde à l'aide du plan AWS Backup Storage. Associez cette politique aux rôles assumés par les instances EC2 exécutant SAP HANA avec l'agent Backint.

Utilisation de cette stratégie

Vous pouvez AWSBackupDataTransferAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 22:48 UTC
- Heure modifiée : 10 novembre 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",

```

```
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupFullAccess

AWSBackupFullAccess est une [politique AWS gérée qui : Cette politique](#) est destinée aux administrateurs de sauvegarde et accorde un accès complet aux opérations de AWS sauvegarde, notamment à la création ou à la modification de plans de sauvegarde, à l'attribution de AWS ressources aux plans de sauvegarde, à la suppression de sauvegardes et à la restauration de sauvegardes.

Utilisation de cette politique

Vous pouvez vous associer AWSBackupFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 novembre 2019, 22:21 UTC
- Heure modifiée : 27 novembre 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Version de la politique

Version de la politique : v17 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "rds:DeleteDBSnapshot",
  "rds:DeleteDBClusterSnapshot"
],
"Resource" : "*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "backup.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "DynamoDbPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DynamoDbDeleteBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DeleteBackup"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
}
},
{
  "Sid" : "EfsFileSystemPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFilesystems"
  ],
}
```

```
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
  },
  {
    "Sid" : "Ec2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ec2:describeAvailabilityZones",
      "ec2:DescribeVpcs",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeImages",
      "ec2:DescribeSubnets",
      "ec2:DescribePlacementGroups",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeAddresses"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Ec2DeletePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot",
      "ec2:DeregisterImage"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ResourceGroupTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetTagKeys",
      "tag:GetTagValues",

```

```
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "StorageGatewayVolumePermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeCachediSCSIVolumes",
    "storagegateway:DescribeStorediSCSIVolumes"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
},
{
  "Sid" : "StorageGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:ListGateways"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:*"
},
{
  "Sid" : "StorageGatewayGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeGatewayInformation",
    "storagegateway:ListVolumes",
    "storagegateway:ListLocalDisks"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
},
{
  "Sid" : "IamRolePermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IamPassRolePermissions",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
```

```
"Resource" : [
  "arn:aws:iam::*:role/*AwsBackup*",
  "arn:aws:iam::*:role/*AWSBackup*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "backup.amazonaws.com",
      "restore-testing.backup.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "AwsOrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : "organizations:DescribeOrganization",
  "Resource" : "*"
},
{
  "Sid" : "KmsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:DescribeKey",
    "kms:GenerateDataKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
```

```
    "StringLike" : {
      "kms:ViaService" : "backup.*.amazonaws.com"
    }
  },
  {
    "Sid" : "SystemManagerCommandPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SystemManagerSendCommandPermissions",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Sid" : "FsxPermissions",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems",
      "fsx:DescribeBackups",
      "fsx:DescribeVolumes",
      "fsx:DescribeStorageVirtualMachines"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "FsxDeletePermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DeleteBackup",
    "Resource" : "arn:aws:fsx:*:*:backup/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "backup.amazonaws.com"
        ]
      }
    }
  }
}
```



```

    }
  }
},
{
  "Sid" : "DirectoryServicePermissions",
  "Effect" : "Allow",
  "Action" : "ds:DescribeDirectories",
  "Resource" : "*"
},
{
  "Sid" : "IamCreateServiceLinkedRolePermissions",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "backup.amazonaws.com",
        "restore-testing.backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "BackupGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:AssociateGatewayToServer",
    "backup-gateway:CreateGateway",
    "backup-gateway>DeleteGateway",
    "backup-gateway>DeleteHypervisor",
    "backup-gateway:DisassociateGatewayFromServer",
    "backup-gateway:ImportHypervisorConfiguration",
    "backup-gateway:ListGateways",
    "backup-gateway:ListHypervisors",
    "backup-gateway:ListTagsForResource",
    "backup-gateway:ListVirtualMachines",
    "backup-gateway:PutMaintenanceStartTime",
    "backup-gateway:TagResource",
    "backup-gateway:TestHypervisorConfiguration",
    "backup-gateway:UntagResource",
    "backup-gateway:UpdateGatewayInformation",
    "backup-gateway:UpdateHypervisor"
  ],

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "BackupGatewayHypervisorPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetHypervisor",
      "backup-gateway:GetHypervisorPropertyMappings",
      "backup-gateway:PutHypervisorPropertyMappings",
      "backup-gateway:StartVirtualMachinesMetadataSync"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
  },
  {
    "Sid" : "BackupGatewayVirtualMachinePermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetVirtualMachine"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  },
  {
    "Sid" : "BackupGatewayGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetBandwidthRateLimitSchedule",
      "backup-gateway:GetGateway",
      "backup-gateway:PutBandwidthRateLimitSchedule"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
  },
  {
    "Sid" : "CloudWatchPermissions",
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  },
  {
    "Sid" : "TimestreamDatabasePermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:ListTables",
      "timestream:ListDatabases"
    ],
  },
```

```
    "Resource" : [
      "arn:aws:timestream:*:*:database/*"
    ]
  },
  {
    "Sid" : "TimestreamPermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3BucketPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Sid" : "RedshiftResourcesPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters",
      "redshift:DescribeClusterSubnetGroups",
      "redshift:DescribeClusterSnapshots",
      "redshift:DescribeSnapshotSchedules"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:cluster:*",
      "arn:aws:redshift:*:*:subnetgroup:*",
      "arn:aws:redshift:*:*:snapshot:*/*",
      "arn:aws:redshift:*:*:snapshotschedule:*"
    ]
  },
  {
    "Sid" : "RedshiftPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeNodeConfigurationOptions",
      "redshift:DescribeOrderableClusterOptions",
      "redshift:DescribeClusterParameterGroups",
      "redshift:DescribeClusterTracks"
    ]
  }
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudFormationStackPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/*"
    ]
  },
  {
    "Sid" : "SystemsManagerForSapPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:GetOperation",
      "ssm-sap:ListDatabases",
      "ssm-sap:GetDatabase",
      "ssm-sap:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ResourceAccessManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ram:GetResourceShareAssociations"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync est une [politique AWS gérée](#) qui : fournit AWS BackupGateway l'autorisation de synchroniser les métadonnées des machines virtuelles en votre nom

Utilisation de cette stratégie

Vous pouvez AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 15 décembre 2022, 19:43 UTC
- Heure modifiée : 15 décembre 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ]
    }
  ],
}
```

```
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  },
  {
    "Sid" : "VMTagPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:TagResource",
      "backup-gateway:UntagResource"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupOperatorAccess

AWSBackupOperatorAccess est une [AWS politique gérée](#) : cette politique accorde aux utilisateurs l'autorisation d'attribuer AWS ressources pour sauvegarder les plans, créer des sauvegardes à la demande et restaurer des sauvegardes. Cette politique n'autorise pas l'utilisateur à créer ou à modifier des plans de sauvegarde ou à supprimer des sauvegardes planifiées après leur création.

Utilisation de cette politique

Vous pouvez joindre AWSBackupOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 18 novembre 2019, 22h23 UTC
- Heure modifiée :6 septembre 2023, 20h45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Version de la politique

Version de la politique : v15(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup>DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",

```

```
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFilesystems"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:describeAvailabilityZones",
    "ec2:DescribeVpcs",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeAddresses"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "tag:GetResources"
  ]
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeCachediSCSIVolumes",
      "storagegateway:DescribeStorediSCSIVolumes"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:ListGateways"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeGatewayInformation",
      "storagegateway:ListVolumes",
      "storagegateway:ListLocalDisks"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles",
      "iam:GetRole"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/*AwsBackup*",
      "arn:aws:iam:*:*:role/*AWSBackup*"
    ],
    "Condition" : {
      "StringLike" : {
```

```
        "iam:PassedToService" : "backup.amazonaws.com"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "organizations:DescribeOrganization",
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "fsx:DescribeBackups",
    "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
    "Effect" : "Allow",
    "Action" : "fsx:DescribeFileSystems",
    "Resource" : "arn:aws:fsx:*:*:file-system/*"
},
{
    "Effect" : "Allow",
    "Action" : "fsx:DescribeVolumes",
    "Resource" : "arn:aws:fsx:*:*:volume/*/*"
},
{
    "Effect" : "Allow",
    "Action" : "fsx:DescribeStorageVirtualMachines",
    "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : "ds:DescribeDirectories",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:ListGateways",
      "backup-gateway:ListHypervisors",
      "backup-gateway:ListTagsForResource",
      "backup-gateway:ListVirtualMachines"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetHypervisor",
      "backup-gateway:GetHypervisorPropertyMappings"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetVirtualMachine"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetBandwidthRateLimitSchedule",
      "backup-gateway:GetGateway"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  },
  },
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "timestream:ListDatabases",
    "timestream:ListTables"
  ],
  "Resource" : [
    "arn:aws:timestream:*:*:database/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "timestream:DescribeEndpoints"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSubnetGroups",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeSnapshotSchedules"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:cluster:*",
    "arn:aws:redshift:*:*:subnetgroup:*",
    "arn:aws:redshift:*:*:snapshot:*/*",
    "arn:aws:redshift:*:*:snapshotschedule:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeNodeConfigurationOptions",
    "redshift:DescribeOrderableClusterOptions",
```

```

    "redshift:DescribeClusterParameterGroups",
    "redshift:DescribeClusterTracks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStacks"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetOperation",
    "ssm-sap:ListDatabases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetDatabase",
    "ssm-sap:ListTagsForResource"
  ],
  "Resource" : "arn:aws:ssm-sap:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWSBackupOrganizationAdminAccess

AWSBackupOrganizationAdminAccess est une [politique AWS gérée](#) qui : Cette politique s'adresse aux administrateurs de sauvegarde qui utilisent la gestion des sauvegardes entre comptes pour gérer les sauvegardes pour l'organisation.

Utilisation de cette stratégie

Vous pouvez AWSBackupOrganizationAdminAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 16:23 UTC
- Heure modifiée : 18 novembre 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "organizations:DisableAWSServiceAccess",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "arn:aws:organizations::*:account/*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:AttachPolicy",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy",
    "organizations:DetachPolicy",
    "organizations:DisablePolicyType",
    "organizations:DescribePolicy",
    "organizations:DescribeEffectivePolicy",
    "organizations:ListPolicies",
    "organizations:EnablePolicyType",
    "organizations:CreatePolicy",
    "organizations:UpdatePolicy",
    "organizations>DeletePolicy"
  ],
}
```

```
"Resource" : "*",
"Condition" : {
  "StringLikeIfExists" : {
    "organizations:PolicyType" : [
      "BACKUP_POLICY"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccountsForParent",
    "organizations:ListAccounts",
    "organizations:DescribeOrganization",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListChildren",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganizationalUnit"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA est une [politique AWS gérée](#) qui : fournit l'autorisation AWS de Backup pour restaurer une sauvegarde de SAP HANA sur Amazon EC2

Utilisation de cette stratégie

Vous pouvez les associer `AWSBackupRestoreAccessForSAPHANA` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 22:43 UTC
- Heure modifiée : 10 novembre 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
```

```
    "ssm-sap:ListDatabases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:BackupDatabase",
    "ssm-sap:RestoreDatabase",
    "ssm-sap:UpdateHanaBackupSettings",
    "ssm-sap:GetDatabase",
    "ssm-sap:ListTagsForResource"
  ],
  "Resource" : "arn:aws:ssm-sap:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupServiceLinkedRolePolicyForBackup

AWSBackupServiceLinkedRolePolicyForBackup est une [politique AWS gérée](#) qui : fournit l'autorisation AWS de sauvegarde pour créer des sauvegardes en votre nom sur l'ensemble AWS des services

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service

- Heure de création : 2 juin 2020, 23:08 UTC
- Heure modifiée : 15 décembre 2023, 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",

```

```

    "ec2:DescribeInstances",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnapshotCopyTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
},
{
  "Sid" : "EC2CreateBackupTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AWSBackupManagedResource"
      ]
    }
  }
},
{
  "Sid" : "EC2CreateTagsPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ]
}

```

```
    ],
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  },
  {
    "Sid" : "EC2RDSDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeSnapshotTierStatus",
      "ec2:DescribeImages",
      "rds:DescribeDBSnapshots",
      "rds:DescribeDBClusterSnapshots"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EBSCopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopySnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopyImage",
    "Resource" : "*"
  },
  {
    "Sid" : "EC2ModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeregisterImage",
      "ec2>DeleteSnapshot",
      "ec2:ModifySnapshotTier"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "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" : "SSMSAPPPermissions",
  "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/*"
    ]
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

AWSBackupServiceLinkedRolePolicyForBackupTest est une [politique AWS gérée](#) qui : fournit l'autorisation AWS Backup pour créer des sauvegardes en votre nom sur l'ensemble AWS des services

Utilisation de de de de de de de

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les politiques politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 12 mai 2020, 17:37 UTC
- Heure modifiée : 12 mai 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON politique J

```
{
```


Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 10 janvier 2019, 21:01 UTC
- Heure modifiée : 15 décembre 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Version de la politique

Version de la politique : v18 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb>CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb>DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
```

```
"Sid" : "DynamoDBBackupPermissions",
"Effect" : "Allow",
"Action" : [
  "rds:AddTagsToResource",
  "rds:ListTagsForResource",
  "rds:DescribeDBSnapshots",
  "rds:CreateDBSnapshot",
  "rds:CopyDBSnapshot",
  "rds:DescribeDBInstances",
  "rds:CreateDBClusterSnapshot",
  "rds:DescribeDBClusters",
  "rds:DescribeDBClusterSnapshots",
  "rds:CopyDBClusterSnapshot",
  "rds:DescribeDBClusterAutomatedBackups"
],
"Resource" : "*"
},
{
  "Sid" : "RDSModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:ModifyDBInstance"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:*"
  ]
},
{
  "Sid" : "RDSClusterPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:ModifyDBCluster"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:cluster:*"
  ]
},
{
  "Sid" : "RDSClusterBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds>DeleteDBClusterAutomatedBackup"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
```

```
  },
  {
    "Sid" : "RDSBackupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:DeleteDBSnapshot",
      "rds:ModifyDBSnapshotAttribute"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:snapshot:awsbackup:*"
    ]
  },
  {
    "Sid" : "RDSClusterModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:DeleteDBClusterSnapshot",
      "rds:ModifyDBClusterSnapshotAttribute"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    ]
  },
  {
    "Sid" : "StorageGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:CreateSnapshot",
      "storagegateway:ListTagsForResource"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "EBSCopyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopySnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : [
```

```
    "ec2:CopyImage"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EBSTagAndDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*::snapshot/*"
},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateImage",
    "ec2:DeregisterImage",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTags",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceCreditSpecifications",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeElasticGpus",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSnapshotTierStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2TagPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:image/*"
},
{
  "Sid" : "EC2ModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
```



```
    "ec2:ModifySnapshotAttribute",
    "ec2:ModifyImageAttribute"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "EBSSnapshotTierPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotTier"
  ],
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "BackupVaultPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:DescribeBackupVault",
    "backup:CopyIntoBackupVault"
  ],
  "Resource" : "arn:aws:backup:*::backup-vault:*"
},
{
  "Sid" : "BackupVaultCopyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:CopyFromBackupVault"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EFSPermissions",
  "Effect" : "Allow",
  "Action" : [
```

```
    "elasticfilesystem:Backup",
    "elasticfilesystem:DescribeTags"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "Sid" : "EBSResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2>DeleteSnapshot",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "KMSDynamoDBPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "dynamodb.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSPermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
```

```
"Action" : "kms:CreateGrant",
"Resource" : "*",
"Condition" : {
  "Bool" : {
    "kms:GrantIsForAWSResource" : "true"
  }
}
},
{
  "Sid" : "KMSDataKeyEC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com"
      ]
    }
  }
}
},
{
  "Sid" : "GetResourcesPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMSendPermissions",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
```

```

    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Sid" : "FsxBackupPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DescribeBackups",
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  },
  {
    "Sid" : "FsxCreateBackupPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:CreateBackup",
    "Resource" : [
      "arn:aws:fsx:*:*:file-system/*",
      "arn:aws:fsx:*:*:backup/*",
      "arn:aws:fsx:*:*:volume/*"
    ]
  },
  {
    "Sid" : "FsxPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DescribeFileSystems",
    "Resource" : "arn:aws:fsx:*:*:file-system/*"
  },
  {
    "Sid" : "FsxVolumePermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DescribeVolumes",
    "Resource" : "arn:aws:fsx:*:*:volume/*"
  },
  {
    "Sid" : "FsxListTagsPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:ListTagsForResource",
    "Resource" : [
      "arn:aws:fsx:*:*:file-system/*",
      "arn:aws:fsx:*:*:volume/*"
    ]
  },
  {
    "Sid" : "FsxDeletePermissions",

```

```
"Effect" : "Allow",
"Action" : "fsx:DeleteBackup",
"Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
  "Sid" : "FsxResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx:ListTagsForResource",
    "fsx:ManageBackupPrincipalAssociations",
    "fsx:CopyBackup",
    "fsx:TagResource"
  ],
  "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
  "Sid" : "DynamodbBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:StartAwsBackupJob",
    "dynamodb:ListTagsOfResource"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "BackupGatewayBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:Backup",
    "backup-gateway:ListTagsForResource"
  ],
  "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
},
{
  "Sid" : "CloudformationStackPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStacks",
    "cloudformation:GetTemplate",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
},
}
```

```
{
  "Sid" : "RedshiftCreatePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:CreateClusterSnapshot",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeTags"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/**",
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftSnapshotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift>DeleteClusterSnapshot"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/**"
  ]
},
{
  "Sid" : "RedshiftPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeClusters"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:CreateTags"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/**"
  ]
},
{
```

```

    "Sid" : "TimestreamResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:StartAwsBackupJob",
      "timestream:GetAwsBackupStatus",
      "timestream:ListTables",
      "timestream:ListDatabases",
      "timestream:ListTagsForResource",
      "timestream:DescribeTable",
      "timestream:DescribeDatabase"
    ],
    "Resource" : [
      "arn:aws:timestream:*:*:database/*"
    ]
  },
  {
    "Sid" : "TimestreamEndpointPermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "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:*:*:*"
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBackupServiceRolePolicyForRestores

AWSBackupServiceRolePolicyForRestores est une [politique AWS gérée](#) qui : fournit à AWS Backup l'autorisation d'effectuer des restaurations en votre nom sur l'ensemble AWS des services. Cette politique inclut les autorisations permettant de créer et de supprimer AWS des ressources, telles que des volumes EBS, des instances RDS et des systèmes de fichiers EFS, qui font partie du processus de restauration.

Utilisation de cette politique

Vous pouvez vous associer AWSBackupServiceRolePolicyForRestores à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 12 janvier 2019, 00:23 UTC
- Heure modifiée : 15 décembre 2023, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Version de la politique

Version de la politique : v20 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb>DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2>DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  ]
}
```

```
  },
  {
    "Sid" : "EC2DescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSnapshotTierStatus"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "StorageGatewayVolumePermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DeleteVolume",
      "storagegateway:DescribeCachediSCSIVolumes",
      "storagegateway:DescribeStorediSCSIVolumes",
      "storagegateway:AddTagsToResource"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "StorageGatewayGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeGatewayInformation",
      "storagegateway:CreateStorediSCSIVolume",
      "storagegateway:CreateCachediSCSIVolume"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
  },
  {
    "Sid" : "StorageGatewayListPermissions",
    "Effect" : "Allow",
```

```

    "Action" : [
      "storagegateway:ListVolumes"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:*"
  },
  {
    "Sid" : "RDSPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances",
      "rds:DescribeDBSnapshots",
      "rds:ListTagsForResource",
      "rds:RestoreDBInstanceFromDBSnapshot",
      "rds>DeleteDBInstance",
      "rds:AddTagsToResource",
      "rds:DescribeDBClusters",
      "rds:RestoreDBClusterFromSnapshot",
      "rds>DeleteDBCluster",
      "rds:RestoreDBInstanceToPointInTime",
      "rds:DescribeDBClusterSnapshots",
      "rds:RestoreDBClusterToPointInTime"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EFSPermissions",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:Restore",
      "elasticfilesystem>CreateFilesystem",
      "elasticfilesystem:DescribeFilesystems",
      "elasticfilesystem>DeleteFilesystem",
      "elasticfilesystem:TagResource"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
  },
  {
    "Sid" : "KMSDescribePermissions",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "*"
  },
  {
    "Sid" : "KMSPermissions",

```

```

    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKey",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "dynamodb.*.amazonaws.com",
          "ec2.*.amazonaws.com",
          "elasticfilesystem.*.amazonaws.com",
          "rds.*.amazonaws.com",
          "redshift.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "KMSCreateGrantPermissions",
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      }
    }
  },
  {
    "Sid" : "EBSSnapshotBlockPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ebs:CompleteSnapshot",
      "ebs:StartSnapshot",
      "ebs:PutSnapshotBlock"
    ],
    "Resource" : "arn:aws:ec2:*::snapshot/*"
  },
  {

```

```
"Sid" : "RDSResourcePermissions",
"Effect" : "Allow",
"Action" : [
  "rds:CreateDBInstance"
],
"Resource" : "arn:aws:rds:*:*:db:*"
},
{
  "Sid" : "EC2DeleteAndRestorePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot",
    "ec2:DeleteTags",
    "ec2:RestoreSnapshotTier"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "EC2CreateTagsScopedPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws:backup:source-resource"
      ]
    }
  }
},
{
  "Sid" : "EC2RunInstancesPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "EC2TerminateInstancesPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*"
  },
  {
    "Sid" : "EC2CreateTagsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "ec2:CreateAction" : [
          "RunInstances",
          "CreateVolume"
        ]
      }
    }
  },
  {
    "Sid" : "FsxPermissions",
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateFileSystemFromBackup"
    ],
    "Resource" : [
      "arn:aws:fsx:*:*:file-system/*",
      "arn:aws:fsx:*:*:backup/*"
    ]
  },
  {
    "Sid" : "FsxTagPermissions",
    "Effect" : "Allow",
    "Action" : [
```

```
    "fsx:DescribeFileSystems",
    "fsx:TagResource"
  ],
  "Resource" : "arn:aws:fsx:*:*:file-system/*"
},
{
  "Sid" : "FsxBackupPermissions",
  "Effect" : "Allow",
  "Action" : "fsx:DescribeBackups",
  "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
  "Sid" : "FsxDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx>DeleteFileSystem",
    "fsx:UntagResource"
  ],
  "Resource" : "arn:aws:fsx:*:*:file-system/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/aws:backup:source-resource" : "false"
    }
  }
},
{
  "Sid" : "FsxDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeVolumes"
  ],
  "Resource" : "arn:aws:fsx:*:*:volume/*"
},
{
  "Sid" : "FsxVolumeTagPermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx>CreateVolumeFromBackup",
    "fsx:TagResource"
  ],
  "Resource" : [
    "arn:aws:fsx:*:*:volume/*"
  ],
  "Condition" : {
```

```

    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws:backup:source-resource"
      ]
    }
  },
  {
    "Sid" : "FsxBackupTagPermissions",
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateVolumeFromBackup",
      "fsx:TagResource"
    ],
    "Resource" : [
      "arn:aws:fsx:*:*:storage-virtual-machine/*",
      "arn:aws:fsx:*:*:backup/*",
      "arn:aws:fsx:*:*:volume/*"
    ]
  },
  {
    "Sid" : "FsxVolumePermissions",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DeleteVolume",
      "fsx:UntagResource"
    ],
    "Resource" : "arn:aws:fsx:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/aws:backup:source-resource" : "false"
      }
    }
  },
  {
    "Sid" : "DSPermissions",
    "Effect" : "Allow",
    "Action" : "ds:DescribeDirectories",
    "Resource" : "*"
  },
  {
    "Sid" : "DynamoDBRestorePermissions",
    "Effect" : "Allow",
    "Action" : [

```



```

    "dynamodb:RestoreTableFromAwsBackup"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "GatewayRestorePermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup-gateway:Restore"
  ],
  "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
},
{
  "Sid" : "CloudformationChangeSetPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:TagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
},
{
  "Sid" : "RedshiftClusterSnapshotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:RestoreFromClusterSnapshot",
    "redshift:RestoreTableFromClusterSnapshot"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:snapshot:*/*",
    "arn:aws:redshift:*:*:cluster:*"
  ]
},
{
  "Sid" : "RedshiftClusterPermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeClusters"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:cluster:*"
  ]
},

```

```
{
  "Sid" : "RedshiftTablePermissions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeTableRestoreStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TimestreamResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:StartAwsRestoreJob",
    "timestream:GetAwsRestoreStatus",
    "timestream:ListTables",
    "timestream:ListTagsForResource",
    "timestream:ListDatabases",
    "timestream:DescribeTable",
    "timestream:DescribeDatabase"
  ],
  "Resource" : [
    "arn:aws:timestream:*:*:database/*"
  ]
},
{
  "Sid" : "TimestreamEndpointPermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:DescribeEndpoints"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup est une [politique AWS gérée](#) qui : Politique contenant les autorisations nécessaires à AWS Backup pour sauvegarder des données dans n'importe quel compartiment S3. Cela inclut l'accès en lecture à tous les objets S3 et tout accès au déchiffrement pour toutes les clés KMS.

Utilisation de cette stratégie

Vous pouvez AWSBackupServiceRolePolicyForS3Backup les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 février 2022, 17:40 UTC
- Heure modifiée : 01 septembre 2022, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:PutTargets",
      "events:DescribeRule",
      "events:EnableRule",
      "events:PutRule",
      "events:RemoveTargets",
      "events:ListTargetsByRule",
      "events:DisableRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "events:ListRules",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "s3.*.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketTagging",
      "s3:GetInventoryConfiguration",
      "s3:ListBucketVersions",
      "s3:ListBucket",
      "s3:GetBucketVersioning",
      "s3:GetBucketLocation",
```

```
    "s3:GetBucketAcl",
    "s3:PutInventoryConfiguration",
    "s3:GetBucketNotification",
    "s3:PutBucketNotification"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectAcl",
    "s3:GetObject",
    "s3:GetObjectVersionTagging",
    "s3:GetObjectVersionAcl",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3::*/*"
},
{
  "Effect" : "Allow",
  "Action" : "s3:ListAllMyBuckets",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore est une [politique AWS gérée](#) qui : Politique contenant les autorisations nécessaires à AWS Backup pour restaurer une sauvegarde S3 dans un compartiment. Cela inclut les autorisations de lecture/écriture sur tous les compartiments S3, ainsi que les autorisations vers GenerateDataKey et DescribeKey pour toutes les clés KMS.

Utilisation de cette stratégie

Vous pouvez les associer `AWSBackupServiceRolePolicyForS3Restore` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 février 2022, 17:39 UTC
- Heure modifiée : 07 février 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBatchFullAccess

AWSBatchFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux ressourcesAWS Batch.

Utilisation de cette stratégie

Vous pouvezAWSBatchFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 décembre 2016, 19:35 UTC
- Heure modifiée : 24 octobre 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
```



```

    "ec2:DescribeVpcs",
    "ec2:DescribeImages",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ecs:DescribeClusters",
    "ecs:Describe*",
    "ecs:List*",
    "eks:DescribeCluster",
    "eks:ListClusters",
    "logs:Describe*",
    "logs:Get*",
    "logs:TestMetricFilter",
    "logs:FilterLogEvents",
    "iam:ListInstanceProfiles",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSBatchServiceRole",
    "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
    "arn:aws:iam::*:role/ecsInstanceRole",
    "arn:aws:iam::*:instance-profile/ecsInstanceRole",
    "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
    "arn:aws:iam::*:role/AWSBatchJobRole*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*Batch*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "batch.amazonaws.com"
    }
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBatchServiceEventTargetRole

AWSBatchServiceEventTargetRoleest une [politiqueAWS gérée qui : Politique](#) visant à activer la cible d' CloudWatch événements pour la soumission de JobAWS Batch

Utilisation de cette stratégie

Vous pouvez les associerAWSBatchServiceEventTargetRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 28 février 2018, 22:31 UTC
- Heure modifiée : 28 février 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBatchServiceRole

`AWSBatchServiceRole` est une [politique AWS gérée](#) qui : rôle de service Policy for AWS Batch qui permet d'accéder aux services connexes, notamment EC2, Autoscaling, le service EC2 Container et Cloudwatch Logs.

Utilisation de cette politique

Vous pouvez vous associer `AWSBatchServiceRole` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 6 décembre 2016, 19:36 UTC
- Heure modifiée : 5 décembre 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
```

```

    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "autoscaling>CreateLaunchConfiguration",
    "autoscaling>CreateAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SetDesiredCapacity",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>CreateOrUpdateTags",
    "autoscaling:SuspendProcesses",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "ecs:DescribeClusters",
    "ecs:DescribeContainerInstances",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTasks",
    "ecs>ListAccountSettings",
    "ecs>ListClusters",
    "ecs>ListContainerInstances",
    "ecs>ListTaskDefinitionFamilies",
    "ecs>ListTaskDefinitions",
    "ecs>ListTasks",
    "ecs>CreateCluster",
    "ecs>DeleteCluster",
    "ecs:RegisterTaskDefinition",
    "ecs:DeregisterTaskDefinition",
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask",
    "ecs:UpdateContainerAgent",
    "ecs:DeregisterContainerInstance",
    "logs>CreateLogGroup",
    "logs>CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : "ecs:TagResource",

```

```
    "Resource" : [
      "arn:aws:ecs:*:*:task/*_Batch_*"
    ]
  },
  {
    "Sid" : "AWSBatchPolicyStatement3",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn",
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement4",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com",
          "autoscaling.amazonaws.com",
          "ecs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement5",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
```

```
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBillingConductorFullAccess

`AWSBillingConductorFullAccess` est une [politique AWS gérée](#) qui : Utilisez la politique `AWSBillingConductorFullAccess` gérée pour autoriser un accès complet à la console AWS Billing Conductor (ABC) et aux API. Cette politique permet aux utilisateurs de répertorier, de créer et de supprimer des ressources ABC.

Utilisation de cette stratégie

Vous pouvez `AWSBillingConductorFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 13 avril 2022, 18:02 UTC
- Heure modifiée : 13 avril 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess est une [politiqueAWS gérée](#) qui : Utilisez la politique AWSBillingConductorReadOnlyAccess gérée pour autoriser l'accès en lecture seule à la consoleAWS Billing Conductor (ABC) et aux API. Cette politique accorde l'autorisation d'afficher et de répertorier toutes les ressources ABC. Elle n'inclut pas la possibilité de créer ou de supprimer des ressources.

Utilisation de cette politique

Vous pouvez `AWSBillingConductorReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 13 avril 2022, 18:02 UTC
- Heure modifiée : 13 avril 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess est une [politique AWS gérée](#) qui : permet aux utilisateurs de consulter les factures sur la console de facturation.

Utilisation de cette politique

Vous pouvez vous associer AWSBillingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 août 2020, 20:08 UTC
- Heure modifiée : 17 janvier 2024, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Sid" : "VisualEditor0",
"Effect" : "Allow",
"Action" : [
  "account:GetAccountInformation",
  "aws-portal:ViewBilling",
  "billing:GetBillingData",
  "billing:GetBillingDetails",
  "billing:GetBillingNotifications",
  "billing:GetBillingPreferences",
  "billing:GetCredits",
  "billing:GetContractInformation",
  "billing:GetIAMAccessPreference",
  "billing:GetSellerOfRecord",
  "billing:ListBillingViews",
  "budgets:ViewBudget",
  "budgets:DescribeBudgetActionsForBudget",
  "budgets:DescribeBudgetAction",
  "budgets:DescribeBudgetActionsForAccount",
  "budgets:DescribeBudgetActionHistories",
  "ce:DescribeCostCategoryDefinition",
  "ce:GetCostAndUsage",
  "ce:ListCostCategoryDefinitions",
  "ce:ListTagsForResource",
  "ce:ListCostAllocationTags",
  "consolidatedbilling:ListLinkedAccounts",
  "consolidatedbilling:GetAccountBillingRole",
  "cur:GetClassicReport",
  "cur:GetClassicReportPreferences",
  "cur:GetUsageReport",
  "cur:DescribeReportDefinitions",
  "freetier:GetFreeTierAlertPreference",
  "freetier:GetFreeTierUsage",
  "invoicing:GetInvoiceEmailDeliveryPreferences",
  "invoicing:GetInvoicePDF",
  "invoicing:ListInvoiceSummaries",
  "payments:GetPaymentInstrument",
  "payments:GetPaymentStatus",
  "payments:ListPaymentPreferences",
  "purchase-orders:GetPurchaseOrder",
  "purchase-orders:ViewPurchaseOrders",
  "purchase-orders:ListPurchaseOrderInvoices",
  "purchase-orders:ListPurchaseOrders",
  "purchase-orders:ListTagsForResource",
  "sustainability:GetCarbonFootprintSummary",
```

```
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM est une [politique AWS gérée](#) qui : Cette politique donne des autorisations pour contrôler les AWS ressources. Par exemple, elle permet de démarrer et d'arrêter les instances EC2 ou RDS en exécutant AWS des scripts Systems Manager (SSM).

Utilisation de cette stratégie

Vous pouvez AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 mai 2022, 19:03 UTC
- Heure modifiée : 25 mai 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBudgetsActionsWithAWSResourceControlAccess

AWSBudgetsActionsWithAWSResourceControlAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet aux actionsAWS budgétaires, y compris l'utilisation des actions budgétaires pour contrôler l'état desAWS ressources de fonctionnement viaAWS Management Console

Utilisation de cette stratégie

Vous pouvezAWSBudgetsActionsWithAWSResourceControlAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 octobre 2020, 17:19 UTC
- Heure modifiée : 15 octobre 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroupsWith",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
```

```
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBudgetsReadOnlyAccess

AWSBudgetsReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à la consoleAWS Budgets via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAWSBudgetsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 octobre 2020, 17:18 UTC
- Heure modifiée : 15 octobre 2020, 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBugBustFullAccess

AWSBugBustFullAccess est une [politique AWS gérée](#) qui : Cette politique IAM accorde aux utilisateurs un accès complet à la AWS BugBust console

Utilisation de cette stratégie

Vous pouvez AWSBugBustFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2021, 07:03 UTC
- Heure modifiée : 22 juillet 2021, 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    }
  ],
  {
```

```
    "Sid" : "AWSBugBustFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "bugbust:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSBugBustSLRCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "bugbust.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBugBustPlayerAccess

AWSBugBustPlayerAccess est une [politique AWS gérée](#) qui : Cette politique IAM autorise les utilisateurs à participer à AWS BugBust des événements

Utilisation de cette stratégie

Vous pouvez AWSBugBustPlayerAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2021, 07:15 UTC
- Heure modifiée : 24 juin 2021, 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
```

```
"Action" : [
  "bugbust:ListBugs",
  "bugbust:ListProfilingGroups",
  "bugbust:JoinEvent",
  "bugbust:GetEvent",
  "bugbust:ListEvents",
  "bugbust:GetJoinEventStatus",
  "bugbust:ListEventScores",
  "bugbust:ListEventParticipants",
  "bugbust:UpdateWorkItem",
  "bugbust:ListPullRequests"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy est une [politique AWS gérée](#) qui : accorde des autorisations pour accéder AWS BugBust aux ressources en votre nom

Utilisation

Cette politique est attachée à un rôle lié au service qui permet à au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher politique à à un utilisateur, un groupe ou un rôle.

Détails

- Type : Politique de rôles liée à un service
- Heure de création : 24 juin 2021, 06:59 UTC

- Heure modifiée : 24 juin 2021, 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par stratégie est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées](#)

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet au AWS Certificate Manager (ACM)

Utilisation de cette stratégie

Vous pouvez les associer AWSCertificateManagerFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 janvier 2016, 17:02 UTC
- Heure modifiée : 17 août 2020, 22h18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "acm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerPrivateCAAuditor

AWSCertificateManagerPrivateCAAuditor est une [politique AWS gérée](#) qui : Fournit à l'auditeur un accès à l'autorité de certification privée du AWS Certificate Manager

Utilisation de cette stratégie

Vous pouvez AWSCertificateManagerPrivateCAAuditor les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 23 octobre 2018, 16:51 UTC
- Heure modifiée : 17 août 2020, 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerPrivateCAFullAccess

AWSCertificateManagerPrivateCAFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à l'autorité de certification privée duAWS Certificate Manager

Utilisation de cette stratégie

Vous pouvez les associerAWSCertificateManagerPrivateCAFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la stratégie

- Type : politiqueAWS gérée
- Heure de création : 23 octobre 2018, 16:54 UTC
- Heure modifiée : 23 octobre 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerPrivateCAPrivilegedUser

AWSCertificateManagerPrivateCAPrivilegedUser est une [politique AWS gérée](#) qui : Fournit aux utilisateurs de certificats un accès privilégié à l'autorité de AWS certification privée de Certificate Manager

Utilisation de cette stratégie

Vous pouvez AWSCertificateManagerPrivateCAPrivilegedUser les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 juin 2019, 17:43 UTC
- Heure modifiée : 20 juin 2019, 17:43 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:RevokeCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:ListPermissions"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerPrivateCAReadOnly

AWSCertificateManagerPrivateCAReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à l'autorité de certification privée du AWS Certificate Manager

Utilisation de cette stratégie

Vous pouvez AWSCertificateManagerPrivateCAReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée

- Heure de création : 23 octobre 2018, 16:57 UTC
- Heure modifiée : 17 août 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerPrivateCAUser

AWSCertificateManagerPrivateCAUser est une [politique AWS gérée](#) qui : Fournit aux utilisateurs de certificats un accès à l'autorité de certification privée de Certificate Manager

Utilisation de cette stratégie

Vous pouvez AWSCertificateManagerPrivateCAUser les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 23 octobre 2018, 16:53 UTC
- Heure modifiée : 20 juin 2019, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
```

```

        "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
        ]
    }
}
},
{
    "Effect" : "Deny",
    "Action" : [
        "acm-pca:IssueCertificate"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition" : {
        "StringNotLike" : {
            "acm-pca:TemplateArn" : [
                "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCertificateManagerReadOnly

AWSCertificateManagerReadOnly est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule au AWS Certificate Manager (ACM).

Utilisation de cette stratégie

Vous pouvez les associer AWSCertificateManagerReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 janvier 2016, 17:07 UTC
- Heure modifiée : 15 mars 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
```

```
    "acm:ListTagsForCertificate",
    "acm:GetAccountConfiguration"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSChatbotServiceLinkedRolePolicy

AWSChatbotServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : Le rôle lié au service utilisé par le AWS Chatbot.

Utilisation des stratégies IAM

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des utilisateurs des groupes ou des rôles.

Détails des détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 18 novembre 2019, 16:39 UTC
- Heure modifiée : 18 novembre 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations des autorisations des autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JAM

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS gérées et évoluer les autorisations de moindre privilège](#)

AWSCleanRoomsFullAccess

AWSCleanRoomsFullAccess est une [politique AWS gérée](#) qui : autorise un accès complet aux ressources des salles AWS blanches et à celles associées Services AWS.

Utilisation de cette politique

Vous pouvez vous associer AWSCleanRoomsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2023, 16:10 UTC
- Heure modifiée : 21 mars 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Action" : [
  "iam:PassRole"
],
"Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "cleanrooms.amazonaws.com"
  }
}
},
{
  "Sid" : "ListRolesToPickServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
},
{
  "Sid" : "ListPoliciesToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListPolicies"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetPolicyToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
}
```

```
  },
  {
    "Sid" : "ConsoleDisplayTables",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetSchema",
      "glue:GetSchemaVersion",
      "glue:BatchGetPartition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsolePickQueryResultsBucketListAll",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SetQueryResultsBucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucketVersions"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
    "Sid" : "WriteQueryResults",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
```

```
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
}
},
{
    "Sid" : "ConsoleDisplayQueryResults",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
},
{
    "Sid" : "EstablishLogDeliveries",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
    }
},
{
    "Sid" : "SetupLogGroupsDescribe",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
    }
},
{
    "Sid" : "SetupLogGroupsCreate",
```

```
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogGroup"
],
"Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "cleanrooms.amazonaws.com"
  }
}
},
{
  "Sid" : "SetupLogGroupsResourcePolicy",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "ConsoleLogSummaryQueryLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:StartQuery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
},
{
  "Sid" : "ConsoleLogSummaryObtainLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:GetQueryResults"
  ],
  "Resource" : "*"
}
]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCleanRoomsFullAccessNoQuerying

AWSCleanRoomsFullAccessNoQuerying est une [AWS politique gérée](#) qui : Permet un accès complet à AWS Ressources de Clean Rooms, à l'exception des requêtes dans le cadre d'une collaboration et de l'accès aux Services AWS.

Utilisation de cette politique

Vous pouvez joindre AWSCleanRoomsFullAccessNoQuerying à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 12 janvier 2023, 16h12 UTC
- Heure de modification : 31 juillet 2023, 20:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

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

```
{
  "Sid" : "CleanRoomsAccess",
  "Effect" : "Allow",
  "Action" : [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
    "cleanrooms:BatchGetSchema",
    "cleanrooms:CreateAnalysisTemplate",
    "cleanrooms:CreateCollaboration",
    "cleanrooms:CreateConfiguredTable",
    "cleanrooms:CreateConfiguredTableAnalysisRule",
    "cleanrooms:CreateConfiguredTableAssociation",
    "cleanrooms:CreateMembership",
    "cleanrooms>DeleteAnalysisTemplate",
    "cleanrooms>DeleteCollaboration",
    "cleanrooms>DeleteConfiguredTable",
    "cleanrooms>DeleteConfiguredTableAnalysisRule",
    "cleanrooms>DeleteConfiguredTableAssociation",
    "cleanrooms>DeleteMember",
    "cleanrooms>DeleteMembership",
    "cleanrooms:GetAnalysisTemplate",
    "cleanrooms:GetCollaborationAnalysisTemplate",
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetConfiguredTable",
    "cleanrooms:GetConfiguredTableAnalysisRule",
    "cleanrooms:GetConfiguredTableAssociation",
    "cleanrooms:GetMembership",
    "cleanrooms:GetProtectedQuery",
    "cleanrooms:GetSchema",
    "cleanrooms:GetSchemaAnalysisRule",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:UpdateAnalysisTemplate",
    "cleanrooms:UpdateCollaboration",
    "cleanrooms:UpdateConfiguredTable",
    "cleanrooms:UpdateConfiguredTableAnalysisRule",
    "cleanrooms:UpdateConfiguredTableAssociation",
    "cleanrooms:UpdateMembership",
```

```
    "cleanrooms:ListTagsForResource",
    "cleanrooms:UntagResource",
    "cleanrooms:TagResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CleanRoomsNoQuerying",
  "Effect" : "Deny",
  "Action" : [
    "cleanrooms:StartProtectedQuery",
    "cleanrooms:UpdateProtectedQuery"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PassServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "ListRolesToPickServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
}
```

```
    "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
  },
  {
    "Sid" : "ListPoliciesToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetPolicyToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
  },
  {
    "Sid" : "ConsoleDisplayTables",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetSchema",
      "glue:GetSchemaVersion",
      "glue:BatchGetPartition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EstablishLogDeliveries",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:ListLogDeliveries"
    ]
  }
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsDescribe",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsCreate",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsResourcePolicy",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeResourcePolicies",
      "logs:PutResourcePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
```

```
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
}
},
{
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
        "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
},
{
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
        "logs:GetQueryResults"
    ],
    "Resource" : "*"
}
]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSCleanRoomsMLFullAccess

AWSCleanRoomsMLFullAccess est une [politique AWS gérée](#) qui : autorise un accès complet aux ressources de AWS Clean Rooms ML et à celles associées Services AWS.

Utilisation de cette politique

Vous pouvez vous associer AWSCleanRoomsMLFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 21:02 UTC
- Heure modifiée : 29 novembre 2023, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Sid" : "CleanRoomsConsoleNavigation",
  "Effect" : "Allow",
  "Action" : [
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetConfiguredAudienceModelAssociation",
    "cleanrooms:GetMembership",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CollaborationMembershipCheck",
  "Effect" : "Allow",
  "Action" : [
    "cleanrooms:ListMembers"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cleanrooms-ml.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AssociateModels",
  "Effect" : "Allow",
  "Action" : [
    "cleanrooms:CreateConfiguredAudienceModelAssociation"
  ]
}

```



```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TagAssociations",
    "Effect" : "Allow",
    "Action" : [
      "cleanrooms:TagResource"
    ],
    "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
  },
  {
    "Sid" : "ListRolesToPickServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:ListRolePolicies",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/cleanrooms-ml*",
      "arn:aws:iam:*:*:role/role/cleanrooms-ml*"
    ]
  },
  {
    "Sid" : "ListPoliciesToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetPolicyToInspectServiceRolePolicy",
    "Effect" : "Allow",

```

```
    "Action" : [
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
  },
  {
    "Sid" : "ConsoleDisplayTables",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetSchema",
      "glue:GetSchemaVersion",
      "glue:BatchGetPartition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsolePickOutputBucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsolePickS3Location",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource" : "arn:aws:s3::*cleanrooms-ml*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccess est une [politique AWS gérée](#) qui : autorise l'accès en lecture seule aux ressources AWS Clean Rooms ML et l'accès en lecture seule aux ressources Clean Rooms associées AWS

Utilisation de cette politique

Vous pouvez vous associer AWSCleanRoomsMLReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 20:55 UTC
- Heure modifiée : 29 novembre 2023, 20h55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CleanRoomsConsoleNavigation",
    "Effect" : "Allow",
    "Action" : [
      "cleanrooms:GetCollaboration",
      "cleanrooms:GetConfiguredAudienceModelAssociation",
      "cleanrooms:GetMembership",
      "cleanrooms:ListAnalysisTemplates",
      "cleanrooms:ListCollaborationAnalysisTemplates",
      "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
      "cleanrooms:ListCollaborations",
      "cleanrooms:ListConfiguredTableAssociations",
      "cleanrooms:ListConfiguredTables",
      "cleanrooms:ListMembers",
      "cleanrooms:ListMemberships",
      "cleanrooms:ListProtectedQueries",
      "cleanrooms:ListSchemas",
      "cleanrooms:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CleanRoomsMLRead",
    "Effect" : "Allow",
    "Action" : [
      "cleanrooms-ml:Get*",
      "cleanrooms-ml:List*"
    ],
    "Resource" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCleanRoomsReadOnlyAccess

AWSCleanRoomsReadOnlyAccess est une [politique AWS gérée](#) qui : autorise l'accès en lecture seule aux ressources AWS Clean Rooms et l'accès en lecture seule aux ressources AWS Glue et Amazon CloudWatch Logs associées.

Utilisation de cette stratégie

Vous pouvez AWSCleanRoomsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 12 janvier 2023, 16:10 UTC
- Heure modifiée : 12 janvier 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloud9Administrator

AWSCloud9Administrator est une [politique AWS gérée](#) qui : fournit un accès administrateur à AWS Cloud9.

Utilisation de cette politique

Vous pouvez vous associer AWSCloud9Administrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:17 UTC
- Heure modifiée : 11 octobre 2023, 12h59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "cloud9.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession",
      "ssm:GetConnectionStatus"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ssm:resourceTag/aws:cloud9:environment" : "*"
      },
      "StringEquals" : {
        "aws:CalledViaFirst" : "cloud9.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/*"
    ]
  }
]
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloud9EnvironmentMember

AWSCloud9EnvironmentMember est une [politique AWS gérée](#) qui : permet d'être invité dans les environnements de développement partagés AWS Cloud9.

Utilisation de cette politique

Vous pouvez vous associer AWSCloud9EnvironmentMember à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:18 UTC
- Heure modifiée : 11 octobre 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "cloud9:GetUserSettings",
  "cloud9:UpdateUserSettings",
  "iam:GetUser",
  "iam:ListUsers"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloud9:DescribeEnvironmentMemberships"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "Null" : {
      "cloud9:UserArn" : "true",
      "cloud9:EnvironmentId" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession",
    "ssm:GetConnectionStatus"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/aws:cloud9:environment" : "*"
    },
    "StringEquals" : {
      "aws:CalledViaFirst" : "cloud9.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
```

```
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:document/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloud9ServiceRolePolicy

AWSCloud9ServiceRolePolicy est une [politique AWS gérée](#) qui : Politique de rôle liée aux services pour AWS Cloud9

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 30 novembre 2017, 13:44 UTC
- Heure modifiée : 17 janvier 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2>DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation>DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    }
  ],
  {
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags"
],
"Resource" : [
  "arn:aws:ec2:*:*:instance/*",
  "arn:aws:ec2:*:*:security-group/*"
],
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/Name" : "aws-cloud9-*"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : [
    "arn:aws:license-manager:*:*:license-configuration:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
```

```
    "arn:aws:iam::*:instance-profile/cloud9/*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloud9SSMInstanceProfile

AWSCloud9SSMInstanceProfile est une [politique AWS gérée](#) qui : Cette politique sera utilisée pour attacher un rôle InstanceProfile qui permettra à Cloud9 d'utiliser le gestionnaire de session SSM pour se connecter à l'instance

Utilisation de cette stratégie

Vous pouvez AWSCloud9SSMInstanceProfile les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 14 mai 2020, 11:40 UTC

- Heure modifiée : 14 mai 2020, 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloud9User

AWSCloud9User est une [politique AWS gérée](#) qui : donne l'autorisation de créer des environnements de développement AWS Cloud9 et de gérer des environnements détenus.

Utilisation de cette politique

Vous pouvez vous associer AWSCloud9User à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:16 UTC
- Heure modifiée : 11 octobre 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloud9:CreateEnvironmentEC2",
      "cloud9:CreateEnvironmentSSH"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "cloud9:OwnerArn" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloud9:GetUserPublicKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "cloud9:UserArn" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloud9:DescribeEnvironmentMemberships"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "Null" : {
        "cloud9:UserArn" : "true",
        "cloud9:EnvironmentId" : "true"
      }
    }
  },
  {

```

```
"Effect" : "Allow",
"Action" : [
  "iam:CreateServiceLinkedRole"
],
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "iam:AWSServiceName" : "cloud9.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession",
    "ssm:GetConnectionStatus"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/aws:cloud9:environment" : "*"
    },
    "StringEquals" : {
      "aws:CalledViaFirst" : "cloud9.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloudFormationFullAccess

AWSCloudFormationFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS CloudFormation.

Utilisation de cette stratégie

Vous pouvez les associer AWSCloudFormationFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 juillet 2019, 21:50 UTC
- Heure modifiée : 26 juillet 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudFormationReadOnlyAccess

AWSCloudFormationReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accèsAWS CloudFormation via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAWSCloudFormationReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 13 novembre 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Les détails des des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 juin 2018, 20:15 UTC
- Heure modifiée : 22 novembre 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des autorisations de moindre privilège etAWS évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège](#)

AWSCloudHSMFullAccess

AWSCloudHSMFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à toutes les ressources CloudHSM.

Utilisation de cette stratégie

Vous pouvez AWSCloudHSMFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudHSMReadOnlyAccess

AWSCloudHSMReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à toutes les ressources CloudHSM.

Utilisation de cette stratégie

Vous pouvezAWSCloudHSMReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudHSMRole

AWSCloudHSMRole est une [politiqueAWS gérée](#) qui : Stratégie par défaut pour le rôle de serviceAWS CloudHSM.

Utilisation de cette stratégie

Vous pouvezAWSCloudHSMRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS CloudMapDiscoverInstanceAccess

AWS CloudMapDiscoverInstanceAccess est une [politique AWS gérée](#) qui : donne accès à l'API de découverte de AWS Cloud cartes.

Utilisation de cette politique

Vous pouvez vous associer `AWSCloudMapDiscoverInstanceAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 00:02 UTC
- Heure modifiée : 20 septembre 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloudMapFullAccess

AWSCloudMapFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à toutes les actions de AWS Cloud la carte.

Utilisation de cette stratégie

Vous pouvez AWSCloudMapFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 23:57 UTC
- Heure modifiée : 29 juillet 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "route53:GetHostedZone",
      "route53:ListHostedZonesByName",
      "route53:CreateHostedZone",
      "route53>DeleteHostedZone",
      "route53:ChangeResourceRecordSets",
      "route53:CreateHealthCheck",
      "route53:GetHealthCheck",
      "route53>DeleteHealthCheck",
      "route53:UpdateHealthCheck",
      "ec2:DescribeVpcs",
      "ec2:DescribeRegions",
      "ec2:DescribeInstances",
      "servicediscovery:*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS CloudMapReadOnlyAccess

AWS CloudMapReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à toutes les actions AWS Cloud cartographiques.

Utilisation de cette politique

Vous pouvez vous associer AWS CloudMapReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 23h45 UTC
- Heure modifiée : 20 septembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloudMapRegisterInstanceAccess

AWSCloudMapRegisterInstanceAccess est une [politique AWS gérée](#) qui : fournit un accès aux actions AWS Cloud cartographiques au niveau du déclarant.

Utilisation de cette politique

Vous pouvez vous associer AWSCloudMapRegisterInstanceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 00:04 UTC
- Heure modifiée : 20 septembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
```

```
    "route53:ListHostedZonesByName",
    "route53:ChangeResourceRecordSets",
    "route53:CreateHealthCheck",
    "route53:GetHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:UpdateHealthCheck",
    "servicediscovery:Get*",
    "servicediscovery:List*",
    "servicediscovery:RegisterInstance",
    "servicediscovery:DeregisterInstance",
    "servicediscovery:DiscoverInstances",
    "servicediscovery:DiscoverInstancesRevision",
    "ec2:DescribeInstances"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCloudShellFullAccess

AWSCloudShellFullAccess est une [politique AWS gérée](#) qui : Autorise l'utilisation AWS CloudShell de toutes les fonctionnalités

Utilisation de cette stratégie

Vous pouvez AWSCloudShellFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 15 décembre 2020, 18:07 UTC
- Heure modifiée : 15 décembre 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudTrail_FullAccess

AWSCloudTrail_FullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet àAWS CloudTrail.

Utilisation de cette stratégie

Vous pouvez `AWSCloudTrail_FullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 octobre 2020, 23:41 UTC
- Heure modifiée : 22 février 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudtrail:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles",
      "iam:GetRolePolicy",
      "iam:GetUser"
    ],
  },
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "cloudtrail.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateKey",
      "kms:CreateAlias",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:ListFunctions"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:ListGlobalTables",
      "dynamodb:ListTables"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudTrail_ReadOnlyAccess

AWSCloudTrail_ReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule àAWS CloudTrail.

Utilisation de cette stratégie

Vous pouvezAWSCloudTrail_ReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de mises à jour de mises à jour de juin 2022, 17:19 UTC
- Heure modifiée : 14 juin 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "cloudtrail:Get*",
  "cloudtrail:Describe*",
  "cloudtrail:List*",
  "cloudtrail:LookupEvents"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy est une [stratégieAWS gérée](#) qui : Cette stratégie est utilisée par le rôle lié au service nommé AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents. CloudWatch utilise ce rôle lié au service pour exécuter les actions deAWS System Manager Incident Manager lorsqu'une CloudWatch alarme passe à l'état ALARM. Cette politique accorde l'autorisation à d'effectuer des incidents en votre nom.

Utilisation politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

détails détails détails détails politiques

- Type : Politique de rôles liée à un service
- Heure de création : 27 avril 2021, 13:30 UTC
- Heure modifiée : 27 avril 2021, 13:30 UTC

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 16 juin 2020, 23:53 UTC
- Heure modifiée : 16 juin 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeArtifactReadOnlyAccess

AWSCodeArtifactReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seuleAWS CodeArtifact via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAWSCodeArtifactReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 juin 2020, 21:23 UTC
- Heure modifiée : 25 juin 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Action" : [
    "codeartifact:Describe*",
    "codeartifact:Get*",
    "codeartifact:List*",
    "codeartifact:ReadFromRepository"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "sts:GetServiceBearerToken",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "sts:AWSServiceName" : "codeartifact.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS CodeBuild via le AWS Management Console. Joignez également AmazonS3ReadOnlyAccess pour fournir un accès au téléchargement, aux artefacts de construction et à joindre IAMFullAccess pour créer et gérer le rôle de service pour CodeBuild.

Utilisation de cette politique

Vous pouvez joindre AWSCodeBuildAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 1 décembre 2016, 19:04 UTC
- Heure modifiée :31 juillet 2023, 23:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

Version de la politique

Version de la politique : v13(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
```

```

    "events:ListTargetsByRule",
    "events:ListRuleNamesByTarget",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "logs:GetLogEvents",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "CWLDeleteLogGroupAccess",
  "Action" : [
    "logs:DeleteLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:CreateConnection",
    "codestar-connections:DeleteConnection",
    "codestar-connections:UpdateConnectionInstallation",
    "codestar-connections:TagResource",

```

```

    "codestar-connections:UntagResource",
    "codestar-connections:ListConnections",
    "codestar-connections:ListInstallationTargets",
    "codestar-connections:ListTagsForResource",
    "codestar-connections:GetConnection",
    "codestar-connections:GetIndividualAccessToken",
    "codestar-connections:GetInstallationUrl",
    "codestar-connections:PassConnection",
    "codestar-connections:StartOAuthHandshake",
    "codestar-connections:UseConnection"
  ],
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",

```

```
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:SetTopicAttributes"
    ],
    "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
  },
  {
    "Sid" : "SNSTopicListAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics",
      "sns:GetTopicAttributes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CodeStarNotificationsChatbotAccess",
    "Effect" : "Allow",
    "Action" : [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess est un [AWS politique gérée](#) qui : Permet d'accéder à AWS CodeBuild via le AWS Management Console, mais ne permet pas CodeBuild administration du projet.

Joignez également `AmazonS3ReadOnlyAccess` pour fournir un accès au téléchargement des artefacts de construction.

Utilisation de cette politique

Vous pouvez joindre `AWSCodeBuildDeveloperAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 1 décembre 2016, 19:02 UTC
- Heure de modification : 31 juillet 2023, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",

```

```

    "codecommit:GetBranch",
    "codecommit:GetCommit",
    "codecommit:GetRepository",
    "codecommit:ListBranches",
    "cloudwatch:GetMetricStatistics",
    "events:DescribeRule",
    "events:ListTargetsByRule",
    "events:ListRuleNamesByTarget",
    "logs:GetLogEvents",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsUserAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:ListConnections",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [

```



```
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSTopicListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:ListMicrosoftTeamsChannelConfigurations"
  ],
  "Resource" : "*"
}
],
"Version" : "2012-10-17"
```

}

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSCodeBuildReadOnlyAccess

AWSCodeBuildReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seuleAWS CodeBuild via leAWS Management Console. Connectez également AmazonS3ReadOnlyAccess pour permettre de télécharger des artefacts de construction.

Utilisation de cette stratégie

Vous pouvez les associerAWSCodeBuildReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2016, 19:03 UTC
- Heure modifiée : 14 septembre 2020, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid" : "CodeStarNotificationsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListEventTypes",
      "codestar-notifications:ListTargets"
    ],
    "Resource" : "*"
  }
],
"Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeCommitFullAccess

AWSCodeCommitFullAccess est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS CodeCommit via le AWS Management Console.

Utilisation de cette politique

Vous pouvez joindre AWSCodeCommitFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 9 juillet 2015, 17:02 UTC
- Heure de modification : 17 juillet 2023, 21h50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Version de la politique

Version de la politique : v10(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
```

```
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListUsers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyConsoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAccessKeys",
    "iam:ListSSHPublicKeys",
    "iam:ListServiceSpecificCredentials"
  ],
  "Resource" : "arn:aws:iam:*:*:user/${aws:username}"
},
{
  "Sid" : "IAMUserSSHKeys",
  "Effect" : "Allow",
  "Action" : [
```

```

    "iam:DeleteSSHPublicKey",
    "iam:GetSSHPublicKey",
    "iam:ListSSHPublicKeys",
    "iam:UpdateSSHPublicKey",
    "iam:UploadSSHPublicKey"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMSelfManageServiceSpecificCredentials",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceSpecificCredential",
    "iam:UpdateServiceSpecificCredential",
    "iam>DeleteServiceSpecificCredential",
    "iam:ResetServiceSpecificCredential"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications>ListNotificationRules",
    "codestar-notifications>ListTargets",
    "codestar-notifications>ListTagsForResource",

```

```

    "codestar-notifications:ListEventTypes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
},
{
  "Sid" : "AmazonCodeGuruReviewerFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "codeguru-reviewer:AssociateRepository",
    "codeguru-reviewer:DescribeRepositoryAssociation",
    "codeguru-reviewer:ListRepositoryAssociations",
    "codeguru-reviewer:DisassociateRepository",
    "codeguru-reviewer:DescribeCodeReview",
    "codeguru-reviewer:ListCodeReviews"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonCodeGuruReviewerSLRCreation",
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/codeguru-reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudWatchEventsManagedRules",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",

```



```
    "events:DeleteRule",
    "events:RemoveTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:ListMicrosoftTeamsChannelConfigurations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarConnectionsReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:ListConnections",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
}
]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSCodeCommitPowerUser

`AWSCodeCommitPowerUser` est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS CodeCommit référentiels, mais n'autorise pas la suppression de référentiels.

Utilisation de cette politique

Vous pouvez joindre `AWSCodeCommitPowerUser` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 9 juillet 2015, 17:06 UTC
- Heure de modification : 17 juillet 2023, 21h49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit>DeleteBranch",
        "codecommit>DeleteFile",
```

```

    "codecommit:Describe*",
    "codecommit:DisassociateApprovalRuleTemplateFromRepository",
    "codecommit:EvaluatePullRequestApprovalRules",
    "codecommit:Get*",
    "codecommit:List*",
    "codecommit:Merge*",
    "codecommit:OverridePullRequestApprovalRules",
    "codecommit:Put*",
    "codecommit:Post*",
    "codecommit:TagResource",
    "codecommit:Test*",
    "codecommit:UntagResource",
    "codecommit:Update*",
    "codecommit:GitPull",
    "codecommit:GitPush"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:DisableRule",
    "events:EnableRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionReadAccess",

```

```
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics",
      "sns:ListSubscriptionsByTopic",
      "sns:GetTopicAttributes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LambdaReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "lambda:ListFunctions"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListUsers"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyConsoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListAccessKeys",
      "iam:ListSSHPublicKeys",
      "iam:ListServiceSpecificCredentials"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "IAMUserSSHKeys",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteSSHPublicKey",
      "iam:GetSSHPublicKey",
      "iam:ListSSHPublicKeys",
      "iam:UpdateSSHPublicKey",
      "iam:UploadSSHPublicKey"
    ],
  },
```

```

    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "IAMSelfManageServiceSpecificCredentials",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceSpecificCredential",
      "iam:UpdateServiceSpecificCredential",
      "iam>DeleteServiceSpecificCredential",
      "iam:ResetServiceSpecificCredential"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "CodeStarNotificationsReadWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:CreateNotificationRule",
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:UpdateNotificationRule",
      "codestar-notifications:Subscribe",
      "codestar-notifications:Unsubscribe"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
      }
    }
  },
  {
    "Sid" : "CodeStarNotificationsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListTargets",
      "codestar-notifications:ListTagsForResource",
      "codestar-notifications:ListEventTypes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonCodeGuruReviewerFullAccess",
    "Effect" : "Allow",

```

```
    "Action" : [
      "codeguru-reviewer:AssociateRepository",
      "codeguru-reviewer:DescribeRepositoryAssociation",
      "codeguru-reviewer:ListRepositoryAssociations",
      "codeguru-reviewer:DisassociateRepository",
      "codeguru-reviewer:DescribeCodeReview",
      "codeguru-reviewer:ListCodeReviews"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonCodeGuruReviewerSLRCreation",
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudWatchEventsManagedRules",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:PutTargets",
      "events>DeleteRule",
      "events:RemoveTargets"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CodeStarNotificationsChatbotAccess",
    "Effect" : "Allow",
    "Action" : [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ]
  }
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CodeStarConnectionsReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWS CodeCommitReadOnly

AWS CodeCommitReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule AWS CodeCommit via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AWS CodeCommitReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 juillet 2015, 17:05 UTC
- Heure modifiée : 18 août 2021, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
    },
  ],
}
```



```
    "Resource" : "*"
  },
  {
    "Sid" : "LambdaReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "lambda:ListFunctions"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListUsers"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyConsoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListSSHPublicKeys",
      "iam:ListServiceSpecificCredentials",
      "iam:ListAccessKeys",
      "iam:GetSSHPublicKey"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "CodeStarConnectionsReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : "arn:aws:codestar-connections::*:connection/*"
  },
  {
    "Sid" : "CodeStarNotificationsReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:DescribeNotificationRule"
    ],
  },
```

```
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codeguru-reviewer:DescribeRepositoryAssociation",
    "codeguru-reviewer:ListRepositoryAssociations",
    "codeguru-reviewer:DescribeCodeReview",
    "codeguru-reviewer:ListCodeReviews"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess est une [politique AWS gérée](#) qui : Permet d'enregistrer et de déployer une révision.

Utilisation de cette stratégie

Vous pouvez AWSCodeDeployDeployerAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 19 mai 2015, 18:18 UTC
- Heure modifiée : 2 avril 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource",
    "codestar-notifications:ListEventTypes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSTopicListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployFullAccess

AWSCodeDeployFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux CodeDeploy ressources.

Utilisation de cette stratégie

Vous pouvez les associerAWSCodeDeployFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 19 mai 2015, 18:13 UTC
- Heure modifiée : 2 avril 2020, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications>DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsForResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "sns:CreateTopic",
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSTopicListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployReadOnlyAccess

AWSCodeDeployReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux CodeDeploy ressources.

Utilisation de cette stratégie

Vous pouvez AWSCodeDeployReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 19 mai 2015, 18:21 UTC
- Heure modifiée : 2 avril 2020, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    }
  ]
}
```



```
    }
  },
  {
    "Sid" : "CodeStarNotificationsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListEventTypes",
      "codestar-notifications:ListTargets"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployRole

AWSCodeDeployRole est un [AWS politique gérée](#) qui : Fournit CodeDeploy accès au service pour développer les balises et interagir avec Auto Scaling en votre nom.

Utilisation de cette politique

Vous pouvez joindre AWSCodeDeployRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 04 mai 2015, 18h05 UTC
- Heure modifiée :16 août 2023, 20h38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

Version de la politique

Version de la politique : v11(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling>DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling>CreateAutoScalingGroup",
        "autoscaling>CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling>DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```
    "ec2:TerminateInstances",
    "tag:GetResources",
    "sns:Publish",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:PutMetricAlarm",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:DeregisterTargets"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWS CodeDeployRoleForCloudFormation

AWS CodeDeployRoleForCloudFormation est une [politique AWS gérée](#) qui : fournit un accès au CodeDeploy service permettant d'invoquer la fonction Lambda en votre nom afin d'effectuer un déploiement bleu/vert via CloudFormation.

Utilisation de cette stratégie

Vous pouvez AWS CodeDeployRoleForCloudFormation les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 mai 2020, 17:12 UTC
- Heure modifiée : 19 mai 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployRoleForECS

`AWSCodeDeployRoleForECS` est une [politique AWS gérée](#) qui : fournit un accès à l'ensemble du CodeDeploy service pour effectuer un déploiement bleu/vert d'ECS en votre nom. Accorde un accès complet aux services de support, tels que l'accès complet à la lecture de tous les objets S3, à l'appel de toutes les fonctions Lambda, à la publication sur toutes les rubriques SNS du compte et à la mise à jour de tous les services ECS.

Utilisation de cette stratégie

Vous pouvez les associer `AWSCodeDeployRoleForECS` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 20:40 UTC
- Heure modifiée : 23 septembre 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
```

```
    "ecs:UpdateServicePrimaryTaskSet",
    "ecs>DeleteTaskSet",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:ModifyRule",
    "lambda:InvokeFunction",
    "cloudwatch:DescribeAlarms",
    "sns:Publish",
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ecs-tasks.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployRoleForECSLimited

AWSCodeDeployRoleForECSLimited est une [politique AWS gérée](#) qui : fournit un accès limité au CodeDeploy service pour effectuer un déploiement bleu/vert d'ECS en votre nom.

Utilisation de cette stratégie

Vous pouvez les associer AWSCodeDeployRoleForECSLimited à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 20:42 UTC
- Heure modifiée : 23 septembre 2019, 22h10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs>DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

```
  },
  {
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners",
      "elasticloadbalancing:ModifyListener",
      "elasticloadbalancing:DescribeRules",
      "elasticloadbalancing:ModifyRule"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    },
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
```



```
"Resource" : [
  "arn:aws:iam::*:role/ecsTaskExecutionRole",
  "arn:aws:iam::*:role/ECSTaskExecution*"
],
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : [
      "ecs-tasks.amazonaws.com"
    ]
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambdaest une [politiqueAWS gérée](#) qui : fournit un accès au CodeDeploy service pour effectuer un déploiement Lambda en votre nom.

Utilisation de cette stratégie

Vous pouvezAWSCodeDeployRoleForLambda les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 28 novembre 2017, 14:05 UTC
- Heure modifiée : 3 décembre 2019, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ],
}
```

```
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeDeployRoleForLambdaLimited

AWSCodeDeployRoleForLambdaLimited est une [politique AWS gérée](#) qui : fournit un accès limité au CodeDeploy service pour effectuer un déploiement Lambda en votre nom.

Utilisation de cette stratégie

Vous pouvez les associer AWSCodeDeployRoleForLambdaLimited à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 17 août 2020, 17:14 UTC
- Heure modifiée : 17 août 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    },
    {
      "Effect" : "Allow"
    }
  ]
}
```

```
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodePipeline_FullAccess

AWSCodePipeline_FullAccess est une [politique AWS gérée](#) qui : fournit un accès complet AWS CodePipeline via le AWS Management Console.

Utilisation de cette politique

Vous pouvez vous associer AWSCodePipeline_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 août 2020, 22:38 UTC
- Heure modifiée : 14 mars 2024, 17:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
```

```

    "s3:ListAllMyBuckets",
    "sns:ListTopics",
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource",
    "codestar-notifications:ListEventTypes",
    "states:ListStateMachines"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "CodePipelineAuthoringAccess"
},
{
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:GetBucketPolicy",
    "s3:GetBucketVersioning",
    "s3:GetObjectVersion",
    "s3:CreateBucket",
    "s3:PutBucketPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3::*:codepipeline-*",
  "Sid" : "CodePipelineArtifactsReadWriteAccess"
},
{
  "Action" : [
    "cloudtrail:PutEventSelectors",
    "cloudtrail:CreateTrail",
    "cloudtrail:GetEventSelectors",
    "cloudtrail:StartLogging"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:cloudtrail::*:trail/codepipeline-source-trail",
  "Sid" : "CodePipelineSourceTrailReadWriteAccess"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/cwe-role-*"
  ]
}

```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "events.amazonaws.com"
        ]
      }
    },
  },
  "Sid" : "EventsIAMPassRole"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "codepipeline.amazonaws.com"
      ]
    }
  },
  "Sid" : "CodePipelineIAMPassRole"
},
{
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:DisableRule",
    "events:RemoveTargets"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:events:*:*:rule/codepipeline-*"
  ],
  "Sid" : "CodePipelineEventsReadWriteAccess"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
```



```

    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:ListMicrosoftTeamsChannelConfigurations"
  ],
  "Resource" : "*"
}
],
"Version" : "2012-10-17"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSCodePipeline_ReadOnlyAccess

AWSCodePipeline_ReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule AWS CodePipeline via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AWSCodePipeline_ReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 août 2020, 22:25 UTC
- Heure modifiée : 3 août 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",

```

```

    "codepipeline:ListTagsForResource",
    "s3:ListAllMyBuckets",
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:GetBucketPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3::*:codepipeline-*"
},
{
  "Sid" : "CodeStarNotificationsReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:DescribeNotificationRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
    }
  }
}
],
"Version" : "2012-10-17"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess est une [politique AWS gérée](#) qui : fournit un accès permettant de visualiser et d'approuver les modifications manuelles pour tous les pipelines

Utilisation de cette stratégie

Vous pouvez AWSCodePipelineApproverAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 juillet 2016, 18:59 UTC
- Heure modifiée : 2 août 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess est une [politiqueAWS gérée](#) qui : fournit un accès à des actions personnalisées permettant d'obtenir des informations détaillées sur les tâches (y compris des informations d'identification temporaires) et de signaler les mises à jour de statutAWS CodePipeline.

Utilisation de cette stratégie

Vous pouvezAWSCodePipelineCustomActionAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 juillet 2015, 17:02 UTC
- Heure modifiée : 09 juillet 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeStarFullAccess

AWSCodeStarFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet àAWS CodeStar via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAWSCodeStarFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 19 avril 2017, 16:23 UTC
- Heure modifiée : 28 mars 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

```
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicyest une [politiqueAWS gérée](#) qui :
AutoriseAWS CodeStar les notifications à accéder à Amazon CloudWatch Events en votre nom

Utilisation des politique de politique de politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles à vos utilisateurs, des groupes ou des rôles.

détails des politique de politique

- Type : Politique de rôles liée à un service
- Heure de création : 5 novembre 2019, 16:10 UTC
- Heure modifiée : 19 mars 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par stratégie est la version qui définit les autorisations pour la politique est la version qui définit les autorisations pour la stratégie qui est celle qui définit les autorisations pour la Lorsqu'un

utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document de politique JSON politique J

```
{
  "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"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégieAWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège de moindre privilège de moindre privilège](#)

AWSCodeStarServiceRole

AWSCodeStarServiceRole est une [politiqueAWS gérée](#) qui : NE PAS UTILISER - Une politique de rôle deAWS CodeStar service qui accorde des privilèges administratifs afin de gérer l'IAM et d'autres ressources de service pour CodeStar le compte du client.

Utilisation de cette stratégie

Vous pouvezAWSCodeStarServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 avril 2017, 15:20 UTC
- Heure modifiée : 20 septembre 2021, 19:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
    }
  ]
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ProjectQuickstarts",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::awscodestar-*/*"
    ]
  },
  {
    "Sid" : "ProjectS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:*"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-codestar-*",
      "arn:aws:s3:::elasticbeanstalk-*"
    ]
  },
  {
    "Sid" : "ProjectServices",
    "Effect" : "Allow",
    "Action" : [
      "codestar:*",
      "codecommit:*",
      "codepipeline:*",
      "codedeploy:*",
      "codebuild:*",
      "autoscaling:*",
      "cloudwatch:Put*",
      "ec2:*",
      "elasticbeanstalk:*",
      "elasticloadbalancing:*",
      "iam:ListRoles",
      "logs:*",
      "sns:*",
      "cloud9:CreateEnvironmentEC2",
      "cloud9>DeleteEnvironment",
      "cloud9:DescribeEnvironment*",
      "cloud9:ListEnvironments"
    ]
  }
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ProjectWorkerRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:GetRole",
      "iam:PassRole",
      "iam:GetRolePolicy",
      "iam:PutRolePolicy",
      "iam:SetDefaultPolicyVersion",
      "iam>CreatePolicy",
      "iam>DeletePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam>CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/CodeStarWorker*",
      "arn:aws:iam::*:policy/CodeStarWorker*",
      "arn:aws:iam::*:instance-profile/awscodestar-*"
    ]
  },
  {
    "Sid" : "ProjectTeamMembers",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachUserPolicy",
      "iam:DetachUserPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyArn" : [
          "arn:aws:iam::*:policy/CodeStar_*"
        ]
      }
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "ProjectRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreatePolicy",
      "iam:DeletePolicy",
      "iam:CreatePolicyVersion",
      "iam:DeletePolicyVersion",
      "iam:ListEntitiesForPolicy",
      "iam:ListPolicyVersions",
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : [
      "arn:aws:iam::*:policy/CodeStar_*"
    ]
  },
  {
    "Sid" : "InspectServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-codestar-service-role",
      "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
    ]
  },
  {
    "Sid" : "IAMLinkRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "cloud9.amazonaws.com"
      }
    }
  }
},
{
```

```
"Sid" : "DescribeConfigRuleForARN",
"Effect" : "Allow",
"Action" : [
  "config:DescribeConfigRules"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "ProjectCodeStarConnections",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectCodeStarConnectionsPassConnections",
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine est une [politique AWS gérée](#) qui : refuse l'accès à certaines actions appliquées par l'AWSéquipe au cas où les informations d'identification d'un utilisateur IAM seraient compromises ou révélées publiquement. Ne supprimez PAS cette politique. Veuillez plutôt suivre les instructions spécifiées dans l'e-mail qui vous a été envoyé concernant cet événement.

Utilisation de cette stratégie

Vous pouvez AWSCompromisedKeyQuarantine les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 août 2020, 18:04 UTC
- Heure modifiée : 11 août 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
```



```
    "iam:ChangePassword",
    "iam:CreateAccessKey",
    "iam:CreateInstanceProfile",
    "iam:CreateLoginProfile",
    "iam:CreateRole",
    "iam:CreateUser",
    "iam:DetachUserPolicy",
    "iam:PutUserPermissionsBoundary",
    "iam:PutUserPolicy",
    "iam:UpdateAccessKey",
    "iam:UpdateAccountPasswordPolicy",
    "iam:UpdateUser",
    "ec2:RequestSpotInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "organizations:CreateAccount",
    "organizations:CreateOrganization",
    "organizations:InviteAccountToOrganization",
    "lambda:CreateFunction",
    "lightsail:Create*",
    "lightsail:Start*",
    "lightsail>Delete*",
    "lightsail:Update*",
    "lightsail:GetInstanceAccessDetails",
    "lightsail:DownloadDefaultKeyPair"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2 est une [politique AWS gérée](#) qui : refuse l'accès à certaines actions appliquées par l'AWSéquipe au cas où les informations d'identification d'un utilisateur IAM seraient compromises ou révélées publiquement. Ne supprimez PAS cette politique. Suivez plutôt les instructions spécifiées dans le dossier d'assistance créé pour vous concernant cet événement.

Utilisation de cette stratégie

Vous pouvez AWSCompromisedKeyQuarantineV2 les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 21 avril 2021, 22:30 UTC
- Heure modifiée : 16 mars 2023, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",

```

```
"iam:AttachGroupPolicy",
"iam:AttachRolePolicy",
"iam:AttachUserPolicy",
"iam:ChangePassword",
"iam:CreateAccessKey",
"iam:CreateInstanceProfile",
"iam:CreateLoginProfile",
"iam:CreatePolicyVersion",
"iam:CreateRole",
"iam:CreateUser",
"iam:DetachUserPolicy",
"iam:PassRole",
"iam:PutGroupPolicy",
"iam:PutRolePolicy",
"iam:PutUserPermissionsBoundary",
"iam:PutUserPolicy",
"iam:SetDefaultPolicyVersion",
"iam:UpdateAccessKey",
"iam:UpdateAccountPasswordPolicy",
"iam:UpdateAssumeRolePolicy",
"iam:UpdateLoginProfile",
"iam:UpdateUser",
"lambda:AddLayerVersionPermission",
"lambda:AddPermission",
"lambda:CreateFunction",
"lambda:GetPolicy",
"lambda:ListTags",
"lambda:PutProvisionedConcurrencyConfig",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:UpdateFunctionCode",
"lightsail:Create*",
"lightsail:Delete*",
"lightsail:DownloadDefaultKeyPair",
"lightsail:GetInstanceAccessDetails",
"lightsail:Start*",
"lightsail:Update*",
"organizations:CreateAccount",
"organizations:CreateOrganization",
"organizations:InviteAccountToOrganization",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:PutLifecycleConfiguration",
```

```

    "s3:PutBucketAcl",
    "s3:PutBucketOwnershipControls",
    "s3:DeleteBucketPolicy",
    "s3:ObjectOwnerOverrideToBucketOwner",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketPolicy",
    "s3:ListAllMyBuckets",
    "ec2:PurchaseReservedInstancesOffering",
    "ec2:AcceptReservedInstancesExchangeQuote",
    "ec2:CreateReservedInstancesListing",
    "savingsplans:CreateSavingsPlan"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSConfigMultiAccountSetupPolicy

AWSConfigMultiAccountSetupPolicy est une [politique AWS gérée](#) qui : Permet à Config d'appeler AWS des services et de déployer des ressources de configuration au sein de l'organisation

Utilisation de de de de de de

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des des des politique

- Type : Politique de rôles liée à un service

- Heure de création : 17 juin 2019, 18:03 UTC
- Heure modifiée : 24 février 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config>DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:PutConformancePack",
      "config>DeleteConformancePack"
    ],
    "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeConformancePackStatus"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "config-conforms.amazonaws.com"
      }
    }
  },
  {
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Effect" : "Allow",

```

```
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ssm.amazonaws.com"
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer AWS avec des autorisations moindre privilège](#)

AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise AWS Config à corriger les ressources non conformes en votre nom.

Utilisation de cette politique de politique de

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des utilisateurs, des groupes ou des rôles.

Détails des politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 18 juin 2019, 21:21 UTC
- Heure modifiée : 18 juin 2019, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON de stratégie

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège de moindre privilège de moindre privilège](#)

AWSConfigRoleForOrganizations

AWSConfigRoleForOrganizations est une [politique AWS gérée](#) qui : Autorise AWS Config à appeler des API d'AWS Organizations en lecture seule

Utilisation de cette stratégie

Vous pouvez AWSConfigRoleForOrganizations les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 mars 2018, 22:53 UTC
- Heure modifiée : 24 novembre 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSConfigRulesExecutionRole

AWSConfigRulesExecutionRole est une [politiqueAWS gérée](#) qui : autorise une fonctionAWS Lambda à accéder à l'APIAWS Config et aux instantanés de configuration queAWS Config fournit régulièrement à Amazon S3. Cet accès est requis par les fonctions qui évaluent les modifications de Config pour les règles de configuration personnalisées.

Utilisation de cette stratégie

Vous pouvezAWSConfigRulesExecutionRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 25 mars 2016, 17:59 UTC
- Heure modifiée : 13 mai 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSConfigServiceRolePolicy

AWSConfigServiceRolePolicy est une [politique AWS gérée](#) qui : autorise Config à appeler AWS des services et à collecter des configurations de ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 30 mai 2018, 23:31 UTC
- Heure modifiée : 22 février 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Version de la politique

Version de la politique : v50 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",

```

```
"acm:DescribeCertificate",
"acm:ListCertificates",
"acm:ListTagsForCertificate",
"airflow:GetEnvironment",
"airflow:ListEnvironments",
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:ListApps",
"amplify:ListBranches",
"amplifyuibuilder:ExportThemes",
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"app-integrations:GetEventIntegration",
"app-integrations:ListEventIntegrationAssociations",
"app-integrations:ListEventIntegrations",
"appconfig:GetApplication",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetExtensionAssociation",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeFlow",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"appmesh:DescribeGatewayRoute",
"appmesh:DescribeMesh",
"appmesh:DescribeRoute",
"appmesh:DescribeVirtualGateway",
"appmesh:DescribeVirtualNode",
"appmesh:DescribeVirtualRouter",
"appmesh:DescribeVirtualService",
```

```
"appmesh:ListGatewayRoutes",
"appmesh:ListMeshes",
"appmesh:ListRoutes",
"appmesh:ListTagsForResource",
"appmesh:ListVirtualGateways",
"appmesh:ListVirtualNodes",
"appmesh:ListVirtualRouters",
"appmesh:ListVirtualServices",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"appstream:DescribeApplications",
"appstream:DescribeDirectoryConfigs",
"appstream:DescribeFleets",
"appstream:DescribeStacks",
"appstream:ListTagsForResource",
"appsync:GetApiCache",
"appsync:GetGraphQLApi",
"appsync:ListGraphQLApis",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"APS:DescribeRuleGroupsNamespace",
"APS:DescribeWorkspace",
"aps:ListRuleGroupsNamespaces",
"aps:ListTagsForResource",
"APS:ListWorkspaces",
"athena:GetDataCatalog",
"athena:GetPreparedStatement",
"athena:GetWorkGroup",
"athena:ListDataCatalogs",
"athena:ListPreparedStatements",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:ListAssessments",
"autoscaling-plans:DescribeScalingPlanResources",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeLaunchConfigurations",
"autoscaling:DescribeLifecycleHooks",
```

```
"autoscaling:DescribePolicies",
"autoscaling:DescribeScheduledActions",
"autoscaling:DescribeTags",
"autoscaling:DescribeWarmPool",
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:DescribeBackupVault",
"backup:DescribeFramework",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
"backup:DescribeReportPlan",
"backup:GetBackupPlan",
"backup:GetBackupSelection",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch:ListTagsForResource",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListTagsForResource",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionsForBudget",
"budgets:ViewBudget",
"cassandra:Select",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
```

```
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListEventDataStores",
"cloudtrail:ListTags",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:DescribeAnomalyDetectors",
"cloudwatch:GetDashboard",
"cloudwatch:GetMetricStream",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"cloudwatch:ListTagsForResource",
"codeartifact:DescribeRepository",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListTagsForResource",
"codebuild:BatchGetReportGroups",
"codebuild:ListReportGroups",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:ListRepositories",
"codecommit:ListTagsForResource",
"codedeploy:GetDeploymentConfig",
```



```
"codeguru-profiler:DescribeProfilingGroup",
"codeguru-profiler:GetNotificationConfiguration",
"codeguru-profiler:GetPolicy",
"codeguru-profiler:ListProfilingGroups",
"codeguru-reviewer:DescribeRepositoryAssociation",
"codeguru-reviewer:ListRepositoryAssociations",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetPrincipalTagAttributeMap",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:DescribeIdentityProvider",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:GetGroup",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config>Select*",
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
```

```
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
"connect:ListTagsForResource",
"connect:ListTaskTemplates",
"connect:ListUsers",
"connect:SearchAvailablePhoneNumbers",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"datasync:DescribeAgent",
"datasync:DescribeLocationEfs",
"datasync:DescribeLocationFsxLustre",
"datasync:DescribeLocationFsxWindows",
"datasync:DescribeLocationHdfs",
"datasync:DescribeLocationNfs",
"datasync:DescribeLocationObjectStorage",
"datasync:DescribeLocationS3",
"datasync:DescribeLocationSmb",
"datasync:DescribeTask",
"datasync:ListAgents",
"datasync:ListLocations",
"datasync:ListTagsForResource",
"datasync:ListTasks",
"dax:DescribeClusters",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
```

```
"dax:DescribeSubnetGroups",
"dax:ListTags",
"detective:ListGraphs",
"detective:ListTagsForResource",
"devicefarm:GetInstanceProfile",
"devicefarm:GetNetworkProfile",
"devicefarm:GetProject",
"devicefarm:GetTestGridProject",
"devicefarm:ListInstanceProfiles",
"devicefarm:ListNetworkProfiles",
"devicefarm:ListProjects",
"devicefarm:ListTagsForResource",
"devicefarm:ListTestGridProjects",
"devops-guru:GetResourceCollection",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"dms:DescribeReplicationInstances",
"dms:DescribeReplicationSubnetGroups",
"dms:DescribeReplicationTaskAssessmentRuns",
"dms:DescribeReplicationTasks",
"dms:ListTagsForResource",
"ds:DescribeDirectories",
"ds:DescribeDomainControllers",
"ds:DescribeEventTopics",
"ds:ListLogSubscriptions",
"ds:ListTagsForResource",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeDhcpOptions",
"ec2:DescribeFleets",
"ec2:DescribeNetworkAcls",
"ec2:DescribePlacementGroups",
"ec2:DescribeRouteTables",
```

```
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeTags",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitionFamilies",
"ecs:ListTaskDefinitions",
"eks:DescribeAddon",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeIdentityProviderConfig",
"eks:DescribeNodegroup",
"eks:ListAddons",
"eks:ListClusters",
"eks:ListFargateProfiles",
```

```
"eks:ListIdentityProviderConfigs",
"eks:ListNodegroups",
"eks:ListTagsForResource",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheParameters",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticache:ListTagsForResource",
"elasticbeanstalk:DescribeConfigurationSettings",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
```

```
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"es:DescribeDomain",
"es:DescribeDomains",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:GetCompatibleElasticsearchVersions",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListTags",
"events:DescribeApiDestination",
"events:DescribeArchive",
"events:DescribeConnection",
"events:DescribeEndpoint",
"events:DescribeEventBus",
"events:DescribeRule",
"events:ListApiDestinations",
"events:ListArchives",
"events:ListConnections",
"events:ListEndpoints",
"events:ListEventBuses",
"events:ListRules",
"events:ListTagsForResource",
"events:ListTargetsByRule",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"finSPACE:GetEnvironment",
"finSPACE:ListEnvironments",
"firehose:DescribeDeliveryStream",
"firehose:ListDeliveryStreams",
"firehose:ListTagsForDeliveryStream",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
```

```
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:ListPolicies",
"fms:ListTagsForResource",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"forecast:ListTagsForResource",
"frauddetector:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetLabels",
"frauddetector:GetModels",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListTagsForResource",
"fsx:DescribeBackups",
"fsx:DescribeDataRepositoryAssociations",
"fsx:DescribeFileSystems",
"fsx:DescribeSnapshots",
"fsx:DescribeStorageVirtualMachines",
"fsx:DescribeVolumes",
"fsx:ListTagsForResource",
"gamelift:DescribeAlias",
"gamelift:DescribeBuild",
"gamelift:DescribeFleetAttributes",
"gamelift:DescribeFleetCapacity",
"gamelift:DescribeFleetLocationAttributes",
"gamelift:DescribeFleetLocationCapacity",
"gamelift:DescribeFleetPortSettings",
"gamelift:DescribeGameServerGroup",
"gamelift:DescribeGameSessionQueues",
"gamelift:DescribeMatchmakingConfigurations",
"gamelift:DescribeMatchmakingRuleSets",
"gamelift:DescribeRuntimeConfiguration",
"gamelift:DescribeScript",
"gamelift:DescribeVpcPeeringAuthorizations",
"gamelift:DescribeVpcPeeringConnections",
"gamelift:ListAliases",
"gamelift:ListBuilds",
```

```
"gamelift:ListFleets",
"gamelift:ListGameServerGroups",
"gamelift:ListScripts",
"gamelift:ListTagsForResource",
"geo:DescribeGeofenceCollection",
"geo:DescribeMap",
"geo:DescribePlaceIndex",
"geo:DescribeRouteCalculator",
"geo:DescribeTracker",
"geo:ListGeofenceCollections",
"geo:ListMaps",
"geo:ListPlaceIndexes",
"geo:ListRouteCalculators",
"geo:ListTrackerConsumers",
"geo:ListTrackers",
"globalaccelerator:DescribeAccelerator",
"globalaccelerator:DescribeEndpointGroup",
"globalaccelerator:DescribeListener",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"globalaccelerator:ListTagsForResource",
"glue:BatchGetDevEndpoints",
"glue:BatchGetJobs",
"glue:BatchGetWorkflows",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobs",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTags",
"glue:GetWorkflow",
```



```
"glue:ListCrawlers",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListWorkflows",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
"greengrass:GetComponent",
"greengrass:ListComponents",
"greengrass:ListComponentVersions",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMissionProfile",
"groundstation:ListConfigs",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListMissionProfiles",
"groundstation:ListTagsForResource",
"guardduty:DescribePublishingDestination",
"guardduty:GetAdministratorAccount",
"guardduty:GetDetector",
"guardduty:GetFilter",
"guardduty:GetFindings",
"guardduty:GetIPSet",
"guardduty:GetMasterAccount",
"guardduty:GetMemberDetectors",
"guardduty:GetMembers",
"guardduty:GetThreatIntelSet",
"guardduty:ListDetectors",
"guardduty:ListFilters",
"guardduty:ListFindings",
"guardduty:ListIPSets",
"guardduty:ListMembers",
"guardduty:ListOrganizationAdminAccounts",
"guardduty:ListPublishingDestinations",
"guardduty:ListTagsForResource",
"guardduty:ListThreatIntelSets",
"healthlake:DescribeFHIRDatastore",
"healthlake:ListFHIRDatastores",
"healthlake:ListTagsForResource",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
```

```
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetInstanceProfile",
"iam:GetOpenIDConnectProvider",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetSAMLProvider",
"iam:GetServerCertificate",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:ListAccessKeys",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedRolePolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListGroupsForUser",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListInstanceProfileTags",
"iam:ListMFADevices",
"iam:ListMFADeviceTags",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicyVersions",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:GetComponent",
"imagebuilder:GetContainerRecipe",
"imagebuilder:GetDistributionConfiguration",
"imagebuilder:GetImage",
"imagebuilder:GetImagePipeline",
"imagebuilder:GetImageRecipe",
"imagebuilder:GetInfrastructureConfiguration",
```

```
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"inspector2:BatchGetAccountStatus",
"inspector2:GetDelegatedAdminAccount",
"inspector2:ListFilters",
"inspector2:ListMembers",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeCustomMetric",
"iot:DescribeDimension",
"iot:DescribeDomainConfiguration",
"iot:DescribeFleetMetric",
"iot:DescribeJobTemplate",
"iot:DescribeMitigationAction",
"iot:DescribeProvisioningTemplate",
"iot:DescribeRoleAlias",
"iot:DescribeScheduledAudit",
"iot:DescribeSecurityProfile",
"iot:GetPolicy",
"iot:GetTopicRule",
"iot:GetTopicRuleDestination",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCustomMetrics",
"iot:ListDimensions",
"iot:ListDomainConfigurations",
"iot:ListFleetMetrics",
"iot:ListJobTemplates",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListScheduledAudits",
"iot:ListSecurityProfiles",
```

```
"iot:ListSecurityProfilesForTarget",
"iot:ListTagsForResource",
"iot:ListTargetsForSecurityProfile",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:ValidateSecurityProfileBehaviors",
"iotanalytics:DescribeChannel",
"iotanalytics:DescribeDataset",
"iotanalytics:DescribeDatastore",
"iotanalytics:DescribePipeline",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotanalytics:ListTagsForResource",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"iotsitewise:DescribeAccessPolicy",
"iotsitewise:DescribeAsset",
"iotsitewise:DescribeAssetModel",
"iotsitewise:DescribeDashboard",
"iotsitewise:DescribeGateway",
"iotsitewise:DescribePortal",
"iotsitewise:DescribeProject",
"iotsitewise:ListAccessPolicies",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListDashboards",
"iotsitewise:ListGateways",
"iotsitewise:ListPortals",
"iotsitewise:ListProjectAssets",
"iotsitewise:ListProjects",
"iotsitewise:ListTagsForResource",
"iottwinmaker:GetComponentType",
"iottwinmaker:GetEntity",
"iottwinmaker:GetScene",
"iottwinmaker:GetSyncJob",
"iottwinmaker:GetWorkspace",
```

```
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListSyncJobs",
"iottwinmaker:ListTagsForResource",
"iottwinmaker:ListWorkspaces",
"iotwireless:GetFuotaTask",
"iotwireless:GetMulticastGroup",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamKey",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreamKeys",
"ivs:ListTagsForResource",
"kafka:DescribeCluster",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:DescribeVpcConnection",
"kafka:GetClusterPolicy",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurations",
"kafka:ListScramSecrets",
"kafka:ListTagsForResource",
"kafka:ListVpcConnections",
"kafkaconnect:DescribeConnector",
"kafkaconnect:ListConnectors",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kendra:ListTagsForResource",
"kinesis:DescribeStreamConsumer",
```

```
"kinesis:DescribeStreamSummary",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListAliases",
"kms:ListKeys",
"kms:ListResourceTags",
"lakeformation:DescribeResource",
"lakeformation:GetDataLakeSettings",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lambda:GetAlias",
"lambda:GetCodeSigningConfig",
"lambda:GetFunction",
"lambda:GetFunctionCodeSigningConfig",
"lambda:GetLayerVersion",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lambda:ListTags",
"lambda:ListVersionsByFunction",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotVersion",
"lex:DescribeResourcePolicy",
"lex:ListBotAliases",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
```

```
"lex:ListTagsForResource",
"license-manager:GetGrant",
"license-manager:GetLicense",
"license-manager:ListDistributedGrants",
"license-manager:ListLicenses",
"license-manager:ListReceivedGrants",
"lightsail:GetAlarms",
"lightsail:GetBuckets",
"lightsail:GetCertificates",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDistributions",
"lightsail:GetInstance",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:GetDataProtectionPolicy",
"logs:GetLogDelivery",
"logs:ListLogDeliveries",
"logs:ListTagsLogGroup",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:DescribeAlert",
"lookoutmetrics:DescribeAnomalyDetector",
"lookoutmetrics:ListAlerts",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutmetrics:ListMetricSets",
"lookoutmetrics:ListTagsForResource",
"lookoutvision:DescribeProject",
"lookoutvision:ListProjects",
"m2:GetEnvironment",
"m2:ListEnvironments",
"m2:ListTagsForResource",
```

```
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetClassificationExportConfiguration",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetMacieSession",
"macie2:ListCustomDataIdentifiers",
"macie2:ListTagsForResource",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNodes",
"mediaconnect:DescribeFlow",
"mediaconnect:ListFlows",
"mediaconnect:ListTagsForResource",
"mediapackage-vod:DescribePackagingConfiguration",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mediapackage-vod:ListTagsForResource",
"mediatailor:GetPlaybackConfiguration",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeAcls",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:DescribeSubnetGroups",
"memorydb:DescribeUsers",
"memorydb:ListTags",
"mobiletargeting:GetApp",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetApps",
"mobiletargeting:GetCampaign",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetEmailChannel",
"mobiletargeting:GetEmailTemplate",
"mobiletargeting:GetEventStream",
"mobiletargeting:GetInAppTemplate",
"mobiletargeting:GetSegment",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTagsForResource",
"mobiletargeting:ListTemplates",
```



```
"mq:DescribeBroker",
"mq:ListBrokers",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectPeer",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetSites",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:ListConnectPeers",
"networkmanager:ListTagsForResource",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetStreamingImage",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStudioComponents",
"nimble:ListStudios",
"opsworks:DescribeInstances",
"opsworks:DescribeLayers",
"opsworks:DescribeTimeBasedAutoScaling",
"opsworks:DescribeVolumes",
"opsworks:ListTags",
"organizations:DescribeAccount",
"organizations:DescribeEffectivePolicy",
"organizations:DescribeOrganization",
"organizations:DescribeOrganizationalUnit",
"organizations:DescribePolicy",
"organizations:DescribeResourcePolicy",
"organizations:ListAccounts",
"organizations:ListAccountsForParent",
"organizations:ListDelegatedAdministrators",
"organizations:ListOrganizationalUnitsForParent",
"organizations:ListParents",
"organizations:ListPolicies",
"organizations:ListPoliciesForTarget",
"organizations:ListRoots",
"organizations:ListTagsForResource",
"organizations:ListTargetsForPolicy",
```

```
"panorama:DescribeApplicationInstance",
"panorama:DescribeApplicationInstanceDetails",
"panorama:DescribePackage",
"panorama:DescribePackageVersion",
"panorama:ListApplicationInstances",
"panorama:ListNodes",
"panorama:ListPackages",
"personalize:DescribeDataset",
"personalize:DescribeDatasetGroup",
"personalize:DescribeSchema",
"personalize:DescribeSolution",
"personalize:ListDatasetGroups",
"personalize:ListDatasetImportJobs",
"personalize:ListDatasets",
"personalize:ListSchemas",
"personalize:ListSolutions",
"personalize:ListTagsForResource",
"profile:GetDomain",
"profile:GetIntegration",
"profile:GetProfileObjectType",
"profile:ListDomains",
"profile:ListIntegrations",
"profile:ListProfileObjectTypes",
"profile:ListTagsForResource",
"quicksight:DescribeAccountSubscription",
"quicksight:DescribeAnalysis",
"quicksight:DescribeAnalysisPermissions",
"quicksight:DescribeDashboard",
"quicksight:DescribeDashboardPermissions",
"quicksight:DescribeDataSet",
"quicksight:DescribeDataSetPermissions",
"quicksight:DescribeDataSetRefreshProperties",
"quicksight:DescribeDataSource",
"quicksight:DescribeDataSourcePermissions",
"quicksight:DescribeTemplate",
"quicksight:DescribeTemplatePermissions",
"quicksight:DescribeTheme",
"quicksight:DescribeThemePermissions",
"quicksight:ListAnalyses",
"quicksight:ListDashboards",
"quicksight:ListDataSets",
"quicksight:ListDataSources",
"quicksight:ListTagsForResource",
"quicksight:ListTemplates",
```

```
"quicksight:ListThemes",
"ram:GetPermission",
"ram:GetResourceShareAssociations",
"ram:GetResourceShares",
"ram:ListPermissionAssociations",
"ram:ListPermissions",
"ram:ListPermissionVersions",
"ram:ListResources",
"ram:ListResourceSharePermissions",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:ListTagsForResource",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEndpointAccess",
"redshift:DescribeEndpointAuthorization",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeLoggingStatus",
```

```
"redshift:DescribeScheduledActions",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"rekognition:DescribeStreamProcessor",
"rekognition:ListStreamProcessors",
"rekognition:ListTagsForResource",
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListTagsForResource",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListTagsForResource",
"resource-groups:GetGroup",
"resource-groups:GetGroupConfiguration",
"resource-groups:GetGroupQuery",
"resource-groups:GetTags",
"resource-groups:ListGroupResources",
"resource-groups:ListGroups",
"robomaker:DescribeRobotApplication",
"robomaker:DescribeSimulationApplication",
"robomaker:ListRobotApplications",
"robomaker:ListSimulationApplications",
"route53-recovery-control-config:DescribeCluster",
"route53-recovery-control-config:DescribeControlPanel",
"route53-recovery-control-config:DescribeRoutingControl",
"route53-recovery-control-config:DescribeSafetyRule",
"route53-recovery-control-config:ListClusters",
"route53-recovery-control-config:ListControlPanels",
"route53-recovery-control-config:ListRoutingControls",
"route53-recovery-control-config:ListSafetyRules",
"route53-recovery-control-config:ListTagsForResource",
"route53-recovery-readiness:GetCell",
"route53-recovery-readiness:GetReadinessCheck",
"route53-recovery-readiness:GetRecoveryGroup",
"route53-recovery-readiness:GetResourceSet",
"route53-recovery-readiness:ListCells",
"route53-recovery-readiness:ListReadinessChecks",
```

```
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53:GetChange",
"route53:GetDNSSEC",
"route53:GetHealthCheck",
"route53:GetHostedZone",
"route53:ListCidrBlocks",
"route53:ListCidrCollections",
"route53:ListCidrLocations",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListQueryLoggingConfigs",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53resolver:GetFirewallDomainList",
"route53resolver:GetFirewallRuleGroup",
"route53resolver:GetFirewallRuleGroupAssociation",
"route53resolver:GetResolverDnssecConfig",
"route53resolver:GetResolverEndpoint",
"route53resolver:GetResolverQueryLogConfig",
"route53resolver:GetResolverQueryLogConfigAssociation",
"route53resolver:GetResolverRule",
"route53resolver:GetResolverRuleAssociation",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallDomains",
"route53resolver:ListFirewallRuleGroupAssociations",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListFirewallRules",
"route53resolver:ListResolverDnssecConfigs",
"route53resolver:ListResolverEndpointIpAddresses",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverQueryLogConfigAssociations",
"route53resolver:ListResolverQueryLogConfigs",
"route53resolver:ListResolverRuleAssociations",
"route53resolver:ListResolverRules",
"route53resolver:ListTagsForResource",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"rum:ListTagsForResource",
"s3-outposts:GetAccessPoint",
"s3-outposts:GetAccessPointPolicy",
"s3-outposts:GetBucket",
```

```
"s3-outposts:GetBucketPolicy",
"s3-outposts:GetBucketTagging",
"s3-outposts:GetLifecycleConfiguration",
"s3-outposts:ListAccessPoints",
"s3-outposts:ListEndpoints",
"s3-outposts:ListRegionalBuckets",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointForObjectLambda",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyForObjectLambda",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccessPointPolicyStatusForObjectLambda",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketNotification",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicy",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketRequestPayment",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetBucketWebsite",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:GetReplicationConfiguration",
"s3:GetStorageLensConfiguration",
"s3:GetStorageLensConfigurationTagging",
"s3:ListAccessPoints",
"s3:ListAccessPointsForObjectLambda",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"s3:ListStorageLensConfigurations",
"s3express:GetBucketPolicy",
"s3express:ListAllMyDirectoryBuckets",
"sagemaker:DescribeAppImageConfig",
```

```
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceExperiment",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribeProject",
"sagemaker:DescribeWorkteam",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListCodeRepositories",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDomains",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListFeatureGroups",
"sagemaker:ListImages",
"sagemaker:ListImageVersions",
"sagemaker:ListInferenceExperiments",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelines",
"sagemaker:ListProjects",
"sagemaker:ListTags",
"sagemaker:ListWorkteams",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
```

```
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"sdb:GetAttributes",
"sdb:ListDomains",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:DescribeHub",
"servicecatalog:DescribePortfolioShares",
"servicediscovery:GetInstance",
"servicediscovery:GetNamespace",
"servicediscovery:GetService",
"servicediscovery:ListInstances",
"servicediscovery:ListNamespaces",
"servicediscovery:ListServices",
"servicediscovery:ListTagsForResource",
"ses:DescribeReceiptRule",
"ses:DescribeReceiptRuleSet",
"ses:GetConfigurationSet",
"ses:GetConfigurationSetEventDestinations",
"ses:GetContactList",
"ses:GetEmailTemplate",
"ses:GetTemplate",
"ses:ListConfigurationSets",
"ses:ListContactLists",
"ses:ListEmailTemplates",
"ses:ListReceiptFilters",
"ses:ListReceiptRuleSets",
"ses:ListTemplates",
"shield:DescribeDRTAccess",
"shield:DescribeProtection",
"shield:DescribeSubscription",
"signer:GetSigningProfile",
"signer:ListProfilePermissions",
"signer:ListSigningProfiles",
"sns:GetDataProtectionPolicy",
"sns:GetSMSSandboxAccountStatus",
"sns:GetSubscriptionAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
```



```
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:DescribeDocumentPermission",
"ssm:DescribeParameters",
"ssm:GetAutomationExecution",
"ssm:GetDocument",
"ssm:ListDocuments",
"ssm:ListTagsForResource",
"sso:DescribeInstanceAccessControlAttributeConfiguration",
"sso:DescribePermissionSet",
"sso:GetInlinePolicyForPermissionSet",
"sso:ListManagedPoliciesInPermissionSet",
"sso:ListPermissionSets",
"sso:ListTagsForResource",
"states:DescribeActivity",
"states:DescribeStateMachine",
"states:ListActivities",
"states:ListStateMachines",
"states:ListTagsForResource",
"storagegateway:ListGateways",
"storagegateway:ListTagsForResource",
"storagegateway:ListVolumes",
"sts:GetCallerIdentity",
"support:DescribeCases",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics:ListAssociatedGroups",
"synthetics:ListGroupResources",
"synthetics:ListGroups",
"synthetics:ListTagsForResource",
"tag:GetResources",
"timestream:DescribeDatabase",
"timestream:DescribeEndpoints",
"timestream:DescribeTable",
"timestream:ListDatabases",
"timestream:ListTables",
```

```

    "timestream:ListTagsForResource",
    "transfer:DescribeAgreement",
    "transfer:DescribeCertificate",
    "transfer:DescribeConnector",
    "transfer:DescribeProfile",
    "transfer:DescribeServer",
    "transfer:DescribeUser",
    "transfer:DescribeWorkflow",
    "transfer:ListAgreements",
    "transfer:ListCertificates",
    "transfer:ListConnectors",
    "transfer:ListProfiles",
    "transfer:ListServers",
    "transfer:ListTagsForResource",
    "transfer:ListUsers",
    "transfer:ListWorkflows",
    "voiceid:DescribeDomain",
    "voiceid:ListTagsForResource",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:GetWebACL",
    "waf-regional:GetWebACLForResource",
    "waf-regional:ListLoggingConfigurations",
    "waf:GetLoggingConfiguration",
    "waf:GetWebACL",
    "wafv2:GetLoggingConfiguration",
    "wafv2:GetRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeTags",
    "workspaces:DescribeWorkspaces"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSConfigSLRLogStatementID",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:CreateLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
},
{

```

```

    "Sid" : "AWSConfigSLRLogEventStatementID",
    "Effect" : "Allow",
    "Action" : "logs:PutLogEvents",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
  },
  {
    "Sid" : "AWSConfigSLRApiGatewayStatementID",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/apis",
      "arn:aws:apigateway:*:*/apis/*",
      "arn:aws:apigateway:*:*/apis/*/integrations",
      "arn:aws:apigateway:*:*/apis/*/integrations/*",
      "arn:aws:apigateway:*:*/domainnames",
      "arn:aws:apigateway:*:*/clientcertificates",
      "arn:aws:apigateway:*:*/clientcertificates/*",
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*/resources/*/methods/*",
      "arn:aws:apigateway:*:*/restapis/*",
      "arn:aws:apigateway:*:*/restapis/*/stages/*",
      "arn:aws:apigateway:*:*/restapis/*/stages",
      "arn:aws:apigateway:*:*/restapis/*/resources",
      "arn:aws:apigateway:*:*/restapis/*/resources/*/methods/*/integration",
      "arn:aws:apigateway:*:*/restapis/*/resources/*",
      "arn:aws:apigateway:*:*/apis/*/routes/*",
      "arn:aws:apigateway:*:*/apis/*/routes",
      "arn:aws:apigateway:*:*/v2/apis/*/routes",
      "arn:aws:apigateway:*:*/v2/apis/*/routes/*",
      "arn:aws:apigateway:*:*/v2/apis",
      "arn:aws:apigateway:*:*/v2/apis/*",
      "arn:aws:apigateway:*:*/v2/apis/*/integrations",
      "arn:aws:apigateway:*:*/v2/apis/*/integrations/*"
    ]
  }
]
}
}
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSConfigUserAccess

`AWSConfigUserAccess` est une [stratégie AWS gérée](#) qui fournit un accès pour utiliser `AWS Config` pour faire des recherches par balise sur des ressources et lire toutes les balises. Cela ne fournit pas l'autorisation de configurer `AWS Config`, qui nécessite des privilèges administratifs.

Utilisation de cette politique

Vous pouvez `AWSConfigUserAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 février 2015, 19:38 UTC
- Heure modifiée : 18 mars 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "config:Get*",
    "config:Describe*",
    "config:Deliver*",
    "config:List*",
    "config:Select*",
    "tag:GetResources",
    "tag:GetTagKeys",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:LookupEvents"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSConnector

AWSConnector est une [politique AWS gérée](#) qui : permet un accès étendu en lecture/écriture à TOUS les objets EC2, un accès en lecture/écriture aux compartiments S3 commençant par « import-to-ec 2 » et la possibilité de répertorier tous les compartiments S3, afin que le Connector puisse importer des machines virtuelles en votre nom. AWS

Utilisation de cette politique

Vous pouvez vous associer AWSConnector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 février 2015, 17:14 UTC
- Heure modifiée : 28 septembre 2015, 19:50 UTC

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

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3>DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
    },
  ],
}
```

```
    "Resource" : "arn:aws:s3:::import-to-ec2-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CancelConversionTask",
      "ec2:CancelExportTask",
      "ec2:CreateImage",
      "ec2:CreateInstanceExportTask",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2>DeleteTags",
      "ec2>DeleteVolume",
      "ec2:DescribeConversionTasks",
      "ec2:DescribeExportTasks",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DetachVolume",
      "ec2:ImportInstance",
      "ec2:ImportVolume",
      "ec2:ModifyInstanceAttribute",
      "ec2:RunInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ImportImage",
      "ec2:DescribeImportImageTasks",
      "ec2:DeregisterImage",
      "ec2:DescribeSnapshots",
      "ec2>DeleteSnapshot",
      "ec2:CancelImportTask",
      "ec2:ImportSnapshot",
      "ec2:DescribeImportSnapshotTasks"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "SNS:Publish"
```

```
    ],
    "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSControlTowerAccountServiceRolePolicy

AWSControlTowerAccountServiceRolePolicy est une [politique AWS gérée](#) qui : permet à AWS Control Tower d'appeler AWS des services qui fournissent une configuration automatique des comptes et une gouvernance centralisée en votre nom.

Utilisation de politiques

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politiques

- Type : Politique de rôle liée à un service
- Heure de création : 5 juin 2023, 22:04 UTC
- Heure modifiée : 5 juin 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events>DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy est une [politique AWS gérée](#) qui : Fournit un accès aux AWS ressources gérées ou utilisées par AWS Control Tower

Utilisation de cette stratégie

Vous pouvez AWSControlTowerServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 3 mai 2019, 18:19 UTC
- Heure modifiée : 12 avril 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation>DeleteStack",
        "cloudformation>DeleteStackInstances",
```

```

    "cloudformation:DeleteStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation>ListStackInstances",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateStackInstances",
    "cloudformation:UpdateStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CreateStackInstances",
    "cloudformation:CreateStackSet",
    "cloudformation>DeleteStack",
    "cloudformation>DeleteStackInstances",
    "cloudformation>DeleteStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:GetTemplate",
    "cloudformation>ListStackInstances",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateStackInstances",
    "cloudformation:UpdateStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
    "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateTrail",

```

```
    "cloudtrail:DeleteTrail",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:StartLogging",
    "cloudtrail:StopLogging",
    "cloudtrail:UpdateTrail",
    "cloudtrail:PutEventSelectors",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
    "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-controltower*/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sts:AssumeRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/AWSControlTowerExecution",
    "arn:aws:iam:*:*:role/AWSControlTowerBlueprintAccess"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:DescribeTrails",
    "ec2:DescribeAvailabilityZones",
    "iam:ListRoles",
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "organizations:CreateAccount",
    "organizations:DescribeAccount",
```

```

    "organizations:DescribeCreateAccountStatus",
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribePolicy",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListParents",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy",
    "organizations:ListRoots",
    "organizations:MoveAccount",
    "servicecatalog:AssociatePrincipalWithPortfolio"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListAttachedRolePolicies",
    "iam:GetRolePolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
    "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
    "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config>DeleteConfigurationAggregator",

```

```
    "config:PutConfigurationAggregator",
    "config:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "config.amazonaws.com",
        "cloudtrail.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "account:EnableRegion",
    "account:ListRegions",
    "account:GetRegionOptStatus"
  ],
  "Resource" : "*"
}
```

```
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicyest une [politiqueAWS gérée](#) qui : accorde les autorisations nécessaires pour décrire l'organisation du compte, créer des compartiments S3 pour le programme MAP et y appliquer des balises, créer un rapport sur les coûts et l'utilisation et décrire les définitions des rapports de coûts et d'utilisation.

Utilisation de cette stratégie

Vous pouvezAWSCostAndUsageReportAutomationPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 novembre 2021, 21:27 UTC
- Heure modifiée : 01 novembre 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataExchangeFullAccess

AWSDataExchangeFullAccess est une [politiqueAWS gérée](#) qui : accorde un accès complet àAWS Data Exchange et auxAWS Marketplace actions à l'aide du SDKAWS Management Console and. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti des échanges deAWS données.

Utilisation de cette politique

Vous pouvezAWSDataExchangeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 2 décembre 2021, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
    "s3:PutObjectAcl"
  ],
  "Resource" : "arn:aws:s3::*aws-data-exchange*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "dataexchange.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:DescribeEntity",
    "aws-marketplace:ListEntities",
    "aws-marketplace:StartChangeSet",
    "aws-marketplace:ListChangeSets",
    "aws-marketplace:DescribeChangeSet",
    "aws-marketplace:CancelChangeSet",
    "aws-marketplace:GetAgreementApprovalRequest",
    "aws-marketplace:ListAgreementApprovalRequests",
    "aws-marketplace:AcceptAgreementApprovalRequest",
    "aws-marketplace:RejectAgreementApprovalRequest",
    "aws-marketplace:UpdateAgreementApprovalRequest",
    "aws-marketplace:SearchAgreements",
    "aws-marketplace:GetAgreementTerms"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:Subscribe",
    "aws-marketplace:Unsubscribe",
```

```
    "aws-marketplace:ViewSubscriptions",
    "aws-marketplace:GetAgreementRequest",
    "aws-marketplace:ListAgreementRequests",
    "aws-marketplace:CancelAgreementRequest"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "redshift:AuthorizeDataShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "redshift:ConsumerIdentifier" : "ADX"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeDataSharesForProducer",
    "redshift:DescribeDataShares"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : "*"
}
]
```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess` est une [politiqueAWS gérée](#) qui : accorde aux fournisseurs de données l'accès àAWS Data Exchange et auxAWS Marketplace actions à l'aide du SDKAWS Management Console et. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti de l'échange deAWS données.

Utilisation de la politique

Vous pouvez `AWSDataExchangeProviderFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 15 mars 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange>Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "arn:aws:s3::*aws-data-exchange*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "dataexchange.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/AWSDataExchange" : "true"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "dataexchange.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource" : "arn:aws:s3::*aws-data-exchange*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "dataexchange.amazonaws.com"
      ]
    }
  }
}
```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:DescribeEntity",
      "aws-marketplace:ListEntities",
      "aws-marketplace:DescribeChangeSet",
      "aws-marketplace:ListChangeSets",
      "aws-marketplace:StartChangeSet",
      "aws-marketplace:CancelChangeSet",
      "aws-marketplace:GetAgreementApprovalRequest",
      "aws-marketplace:ListAgreementApprovalRequests",
      "aws-marketplace:AcceptAgreementApprovalRequest",
      "aws-marketplace:RejectAgreementApprovalRequest",
      "aws-marketplace:UpdateAgreementApprovalRequest",
      "aws-marketplace:SearchAgreements",
      "aws-marketplace:GetAgreementTerms"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
      "kms:ListKeys"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "redshift:AuthorizeDataShare"
    ],
    "Resource" : "*",
```

```
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "redshift:ConsumerIdentifier" : "ADX"
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataExchangeReadOnly

`AWSDataExchangeReadOnly` est une [politiqueAWS gérée](#) qui : accorde un accès en lecture seule àAWS Data Exchange et auxAWS Marketplace actions à l'aide du SDKAWS Management Console and.

Utilisation de cette stratégie

Vous pouvez `AWSDataExchangeReadOnly` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 10 mai 2021, 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",

```

```
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataExchangeSubscriberFullAccess

AWSDataExchangeSubscriberFullAccess est une [politiqueAWS gérée](#) qui : accorde aux abonnés l'accès àAWS Data Exchange et auxAWS Marketplace actions à l'aide du SDKAWS Management Console et. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti des échanges deAWS données.

Utilisation de cette politique

Vous pouvez les associerAWSDataExchangeSubscriberFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 29 novembre 2021, 23 h 00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange>DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
    }
  ]
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3::*aws-data-exchange*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe",
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:GetAgreementRequest",
      "aws-marketplace:ListAgreementRequests",
      "aws-marketplace:CancelAgreementRequest"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
      "kms:ListKeys"
    ],
    "Resource" : "*"
  }
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole` est une [politiqueAWS gérée](#) qui : fournit les autorisations appropriées àAWS Data Lifecycle Manager pour prendre des mesures sur lesAWS ressources

Utilisation de cette stratégie

Vous pouvez `AWSDataLifecycleManagerServiceRole` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 juillet 2018, 19:34 UTC
- Heure modifiée : 19 septembre 2022, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

`AWSDataLifecycleManagerServiceRoleForAMIManagement` est une [politique AWS gérée](#) qui : fournit les autorisations appropriées à AWS Data Lifecycle Manager pour prendre des mesures sur les AWS ressources à des fins de gestion des AMI

Utilisation de cette stratégie

Vous pouvez `AWSDataLifecycleManagerServiceRoleForAMIManagement` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 21 octobre 2020, 19:39 UTC
- Heure modifiée : 19 août 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2>DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataLifecycleManagerSSMFullAccess

AWSDataLifecycleManagerSSMFullAccess est une [politique AWS gérée](#) qui : fournit à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions de Systems Manager requises pour exécuter des pré-scripts et des post-scripts sur toutes les instances Amazon EC2.

Utilisation de cette politique

Vous pouvez vous associer AWSDataLifecycleManagerSSMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 31 octobre 2023, 20:29 UTC
- Heure modifiée : 16 novembre 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
```

```
"Action" : [
  "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ssm:GetDocument"
],
"Resource" : [
  "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
  "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
]
},
{
  "Sid" : "AllowAllEC2Instances",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSDataPipeline_FullAccess

AWSDataPipeline_FullAccess est une [politique AWS gérée](#) qui : fournit un accès complet au Data Pipeline, un accès aux listes pour les rôles S3, DynamoDB, Redshift, RDS, SNS et IAM, et un accès PassRole pour les rôles par défaut.

Utilisation de cette stratégie

Vous pouvez AWSDataPipeline_FullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 19 janvier 2017, 23:14 UTC
- Heure modifiée : 17 août 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataPipeline_PowerUser

AWSDataPipeline_PowerUser est une [politique AWS gérée](#) qui : fournit un accès complet au Data Pipeline, un accès aux listes pour les rôles S3, DynamoDB, Redshift, RDS, SNS et IAM, et un accès PassRole pour les rôles par défaut.

Utilisation de la présente stratégie

Vous pouvez AWSDataPipeline_PowerUser les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 19 janvier 2017, 23:16 UTC
- Heure modifiée : 17 août 2017, 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataSyncDiscoveryServiceRolePolicy

AWSDataSyncDiscoveryServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet à DataSync Discovery de s'intégrer à d'autresAWS services en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 20 mars 2023, 22:19 UTC
- Heure modifiée : 20 mars 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDataSyncFullAccess

AWSDataSyncFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet AWS DataSync et un accès minimal à ses dépendances

Utilisation de cette politique

Vous pouvez vous associer AWSDataSyncFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 19:40 UTC
- Heure modifiée : 16 février 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "datasync:*",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:ModifyNetworkInterfaceAttribute",
    "fsx:DescribeFileSystems",
    "fsx:DescribeStorageVirtualMachines",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "iam:GetRole",
    "iam:ListRoles",
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "logs:DescribeResourcePolicies",
    "outposts:ListOutposts",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3-outposts:ListAccessPoints",
    "s3-outposts:ListRegionalBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DataSyncPassRolePermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "datasync.amazonaws.com"
      ]
    }
  }
}
}
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSDataSyncReadOnlyAccess

AWSDataSyncReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à AWS DataSync

Utilisation de cette stratégie

Vous pouvez AWSDataSyncReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 19:18 UTC
- Heure modifiée : 30 juin 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "datasync:Describe*",
      "datasync:List*",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:DescribeMountTargets",
      "fsx:DescribeFileSystems",
      "iam:GetRole",
      "iam:ListRoles",
      "logs:DescribeLogGroups",
      "logs:DescribeResourcePolicies",
      "s3:ListAllMyBuckets",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepLensLambdaFunctionAccessPolicy

AWSDeepLensLambdaFunctionAccessPolicy est une [politique AWS gérée](#) qui : Cette politique spécifie les autorisations requises par les fonctions Lambda DeepLens administratives qui s'exécutent sur un DeepLens appareil

Utilisation de cette stratégie

Vous pouvez `AWSDeepLensLambdaFunctionAccessPolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 15:47 UTC
- Heure modifiée : 11 juin 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3objectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogStream",
  "logs:DescribeLogStreams",
  "logs:PutLogEvents",
  "logs:CreateLogGroup"
],
"Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
},
{
  "Sid" : "DeepLensAccess",
  "Effect" : "Allow",
  "Action" : [
    "deeplens:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensKinesisVideoAccess",
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:DescribeStream",
    "kinesisvideo:CreateStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:PutMedia"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepLensServiceRolePolicy

AWSDeepLensServiceRolePolicy est une [politique AWS gérée](#) qui : accorde AWS DeepLens l'accès aux Services AWS ressources et aux rôles nécessaires DeepLens et à ses dépendances, notamment à l'IoT, à S3 GreenGrass et AWS Lambda.

Utilisation de cette stratégie

Vous pouvez AWSDeepLensServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 29 novembre 2017, 15:46 UTC
- Heure modifiée : 25 septembre 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",

```

```
    "iot:UpdateThingShadow"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/deeplens*"
  ]
},
{
  "Sid" : "DeepLensIoTCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal",
    "iot:UpdateCertificate",
    "iot>DeleteCertificate",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/deeplens*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/deeplens*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
}
```

```
{
  "Sid" : "DeepLensIoTDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:GetThingShadow",
    "iot:UpdateThingShadow"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/deeplens*"
  ]
},
{
  "Sid" : "DeepLensIoTEndpointAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeEndpoint"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensAccess",
  "Effect" : "Allow",
  "Action" : [
    "deeplens:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensS3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*:deeplens*"
  ]
},
{
  "Sid" : "DeepLensS3Buckets",
  "Effect" : "Allow",
```

```
"Action" : [
  "s3:DeleteBucket",
  "s3:ListBucket"
],
"Resource" : [
  "arn:aws:s3:::deeplens*"
]
},
{
  "Sid" : "DeepLensCreateS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensIAMPassRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "greengrass.amazonaws.com",
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DeepLensIAMLambdaPassRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSDeepLens*",

```

```
    "arn:aws:iam::*:role/service-role/AWSDeepLens*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Sid" : "DeepLensGreenGrassAccess",
  "Effect" : "Allow",
  "Action" : [
    "greengrass:AssociateRoleToGroup",
    "greengrass:AssociateServiceRoleToAccount",
    "greengrass>CreateResourceDefinition",
    "greengrass>CreateResourceDefinitionVersion",
    "greengrass>CreateCoreDefinition",
    "greengrass>CreateCoreDefinitionVersion",
    "greengrass>CreateDeployment",
    "greengrass>CreateFunctionDefinition",
    "greengrass>CreateFunctionDefinitionVersion",
    "greengrass>CreateGroup",
    "greengrass>CreateGroupCertificateAuthority",
    "greengrass>CreateGroupVersion",
    "greengrass>CreateLoggerDefinition",
    "greengrass>CreateLoggerDefinitionVersion",
    "greengrass>CreateSubscriptionDefinition",
    "greengrass>CreateSubscriptionDefinitionVersion",
    "greengrass>DeleteCoreDefinition",
    "greengrass>DeleteFunctionDefinition",
    "greengrass>DeleteGroup",
    "greengrass>DeleteLoggerDefinition",
    "greengrass>DeleteSubscriptionDefinition",
    "greengrass:DisassociateRoleFromGroup",
    "greengrass:DisassociateServiceRoleFromAccount",
    "greengrass:GetAssociatedRole",
    "greengrass:GetConnectivityInfo",
    "greengrass:GetCoreDefinition",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetDeploymentStatus",
    "greengrass:GetDeviceDefinition",
    "greengrass:GetDeviceDefinitionVersion",
    "greengrass:GetFunctionDefinition",
    "greengrass:GetFunctionDefinitionVersion",
```

```
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
"greengrass:ListGroups",
"greengrass:ListLoggerDefinitionVersions",
"greengrass:ListLoggerDefinitions",
"greengrass:ListSubscriptionDefinitionVersions",
"greengrass:ListSubscriptionDefinitions",
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
"greengrass:UpdateFunctionDefinition",
"greengrass:UpdateGroup",
"greengrass:UpdateGroupCertificateConfiguration",
"greengrass:UpdateLoggerDefinition",
"greengrass:UpdateSubscriptionDefinition",
"greengrass:UpdateResourceDefinition"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "DeepLensLambdaAdminFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
```

```
    "lambda:DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:deeplens*"
  ]
},
{
  "Sid" : "DeepLensLambdaUsersFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*"
  ]
},
{
  "Sid" : "DeepLensSageMakerWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateTrainingJob",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:StopTrainingJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/deeplens*"
  ]
},
{
  "Sid" : "DeepLensSageMakerReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribeTrainingJob"
  ]
},
```

```
    "Resource" : [
      "arn:aws:sagemaker:*:*:training-job/*"
    ]
  },
  {
    "Sid" : "DeepLensKinesisVideoStreamAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:CreateStream",
      "kinesisvideo:DescribeStream",
      "kinesisvideo>DeleteStream"
    ],
    "Resource" : [
      "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
    ]
  },
  {
    "Sid" : "DeepLensKinesisVideoEndpointAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:GetDataEndpoint"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess est une [politique AWS gérée](#) qui : l'accès de l' DeepRacer administrateur à toutes les actions, y compris le basculement entre le mode multi-utilisateur et le mode mono-utilisateur.

Utilisation de cette stratégie

Vous pouvez AWSDeepRacerAccountAdminAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 octobre 2021, 01:27 UTC
- Heure modifiée : 28 octobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    ],
    "Condition" : {
      "Null" : {
        "depracer:UserToken" : "true"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerCloudFormationAccessPolicy

AWSDeepRacerCloudFormationAccessPolicyest une [politiqueAWS gérée](#) qui : Permet CloudFormation de créer et de gérer desAWS piles et des ressources en votre nom.

Utilisation de cette stratégie

Vous pouvezAWSDeepRacerCloudFormationAccessPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 février 2019, 21:59 UTC
- Heure modifiée : 14 juin 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteInternetGateway",
        "ec2>DeleteNatGateway",
        "ec2>DeleteNetworkAcl",
        "ec2>DeleteNetworkAclEntry",
        "ec2>DeleteRoute",
        "ec2>DeleteRouteTable",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteSubnet",
```

```

    "ec2:DeleteTags",
    "ec2:DeleteVpc",
    "ec2:DeleteVpcEndpoints",
    "ec2:DescribeAddresses",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:DetachInternetGateway",
    "ec2:DisassociateRouteTable",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ReleaseAddress",
    "ec2:ReplaceNetworkAclAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
  "Condition" : {
    "StringLikeIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:GetFunction",
    "lambda>DeleteFunction",
    "lambda:TagResource",
    "lambda:UpdateFunctionCode"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:*DeepRacer*",
      "arn:aws:lambda:*:*:function:*Deepracer*",
      "arn:aws:lambda:*:*:function:*deepracer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutBucketPolicy",
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3>DeleteBucket"
    ],
    "Resource" : [
      "arn:aws:s3::*:*DeepRacer*",
      "arn:aws:s3::*:*Deepracer*",
      "arn:aws:s3::*:*deepracer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "robomaker:CreateSimulationApplication",
      "robomaker:CreateSimulationApplicationVersion",
      "robomaker>DeleteSimulationApplication",
      "robomaker:DescribeSimulationApplication",
      "robomaker:ListSimulationApplications",
      "robomaker:TagResource",
      "robomaker:UpdateSimulationApplication"
    ],
    "Resource" : [
      "arn:aws:robomaker:*:*:/createSimulationApplication",
      "arn:aws:robomaker:*:*:simulation-application/deepracer*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess est une [politiqueAWS gérée](#) qui : Accès utilisateur DeepRacer MultiUser par défaut pour utiliser Deepracer en mode multi-utilisateurs

Utilisation de cette stratégie

Vous pouvezAWSDeepRacerDefaultMultiUserAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 octobre 2021, 01:27 UTC
- Heure modifiée : 28 octobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "deepracer:Add*",
    "deepracer:Remove*",
    "deepracer:Create*",
    "deepracer:Perform*",
    "deepracer:Clone*",
    "deepracer:Get*",
    "deepracer:List*",
    "deepracer:Edit*",
    "deepracer:Start*",
    "deepracer:Set*",
    "deepracer:Update*",
    "deepracer>Delete*",
    "deepracer:Stop*",
    "deepracer:Import*",
    "deepracer:Tag*",
    "deepracer:Untag*"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "Null" : {
      "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" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerFullAccess

AWSDeepRacerFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS DeepRacer. Fournit également un accès sélectif aux services connexes (par exemple, S3).

Utilisation de cette stratégie

Vous pouvez les associer AWSDeepRacerFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 5 octobre 2020, 22:03 UTC
- Heure modifiée : 5 octobre 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3::*DeepRacer*",
        "arn:aws:s3::*Deepracer*",
        "arn:aws:s3::*depracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3::*DeepRacer*/*",
        "arn:aws:s3::*Deepracer*/*",
        "arn:aws:s3::*depracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicyest une [politiqueAWS gérée](#) qui : Permet RoboMaker de créer les ressources requises et d'appelerAWS des services en votre nom.

Utilisation de cette stratégie

Vous pouvez les associerAWSDeepRacerRoboMakerAccessPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 28 février 2019, 21:59 UTC
- Heure modifiée : 28 février 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",

```

```

    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*DeepRacer*",
    "arn:aws:s3:::*Deepracer*",
    "arn:aws:s3:::*deepracer*",
    "arn:aws:s3:::dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/DeepRacer" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:CreateStream",
    "kinesisvideo:DescribeStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:PutMedia",
    "kinesisvideo:TagStream"
  ],
  "Resource" : [
    "arn:aws:kinesisvideo:*:*:stream/dr-*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy est une [politiqueAWS gérée](#) qui : Permet DeepRacer de créer les ressources requises et d'appelerAWS des services en votre nom.

Utilisation de cette stratégie

Vous pouvezAWSDeepRacerServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 28 février 2019, 21:58 UTC
- Heure modifiée : 12 juin 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "robomaker:*",
    "sagemaker:*",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DetectStackDrift",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:DescribeStackResourceDrifts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "robomaker.amazonaws.com"
    }
  },
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSDeepRacer*",
    "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
  ]
}
```

```
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:InvokeFunction",
    "lambda:UpdateFunctionCode"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*DeepRacer*",
    "arn:aws:lambda:*:*:function:*Deepracer*",
    "arn:aws:lambda:*:*:function:*deepracer*",
    "arn:aws:lambda:*:*:function:*dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutBucketPolicy",
    "s3:GetBucketAcl"
  ],
  "Resource" : [
    "arn:aws:s3::*:*DeepRacer*",
    "arn:aws:s3::*:*Deepracer*",
    "arn:aws:s3::*:*deepracer*",

```

```
    "arn:aws:s3:::dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/DeepRacer" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:CreateStream",
    "kinesisvideo>DeleteStream",
    "kinesisvideo:DescribeStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:GetHLSStreamingSessionURL",
    "kinesisvideo:GetMedia",
    "kinesisvideo:PutMedia",
    "kinesisvideo:TagStream"
  ],
  "Resource" : [
    "arn:aws:kinesisvideo:*:*:stream/dr-*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDenyAll

AWSDenyAll est une [politique AWS gérée](#) qui : Refuse tout accès.

Utilisation de cette politique

Vous pouvez vous associer AWSDenyAll à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 mai 2019, 22:36 UTC
- Heure modifiée : 18 décembre 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSDeviceFarmFullAccess

AWSDeviceFarmFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à toutes les opérations de AWS Device Farm.

Utilisation de cette stratégie

Vous pouvez AWSDeviceFarmFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 13 juillet 2015, 16:37 UTC
- Heure modifiée : 13 juillet 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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


Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
        "aws:RequestTag/AWSDeviceFarmManaged" : "true"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : "CreateNetworkInterface"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
    ],
}
```

```
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluer les autorisations de moindre privilège privilège privilège privilège privilège avec politiques gérées et évoluer les autorisations](#)

AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy est une [politique AWS gérée](#) qui : autorise AWS Device Farm à appeler les API EC2 en votre nom.

Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles

Les détails

- Type : Politique de rôles liée à un service
- Heure de création : 26 mai 2021
- Heure modifiée : 26 mai 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie Lorsque un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
}
```



```
    }  
  }  
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers évoluez vers évoluez vers évoluez vers évoluez vers évoluez vers évoluez](#)

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` est une [politiqueAWS gérée](#) qui : Fournit un accès complet àAWS Direct Connect via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez `AWSDirectConnectFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 30 avril 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDirectConnectReadOnlyAccess

AWSDirectConnectReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule àAWS Direct Connect via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAWSDirectConnectReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC

- Heure modifiée : 18 mai 2020, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDirectConnectServiceRolePolicy

AWSDirectConnectServiceRolePolicy est une [politique AWS gérée](#) qui : fournit l'autorisation AWS Direct Connect pour créer et gérer AWS des ressources en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles attachés à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 14 janvier 2021, 18:35 UTC
- Heure modifiée : 14 janvier 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

```
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:*directconnect*"
  ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDirectoryServiceFullAccess

AWSDirectoryServiceFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet auAWS Directory Service.

Utilisation de cette stratégie

Vous pouvezAWSDirectoryServiceFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 24 novembre 2020, 23h24 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ]
    }
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
  },
  {
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "ds.amazonaws.com"
      }
    }
  },
  {
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDirectoryServiceReadOnlyAccess

AWSDirectoryServiceReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule au AWS Directory Service.

Utilisation de cette stratégie

Vous pouvez AWSDirectoryServiceReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 25 septembre 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
```



```
    "ec2:DescribeVpcs",
    "sns:ListTopics",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDiscoveryContinuousExportFirehosePolicy

AWSDiscoveryContinuousExportFirehosePolicy est une [politique AWS gérée](#) qui : Fournit un accès en écriture aux AWS ressources requises pour AWS Discovery Continuous Export

Utilisation de cette stratégie

Vous pouvez AWSDiscoveryContinuousExportFirehosePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 août 2018, 18:29 UTC
- Heure modifiée : 8 juin 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-stream:*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet à DMS Fleet Advisor de gérer CloudWatch les indicateurs en votre nom.

Utilisation des politiques de cette politique de

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à des utilisateurs, des groupes ou des rôles des stratégies de politique attachée à des stratégies de politique d'utilisateurs,

Détails des politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 6 mars 2023, 09:10 UTC
- Heure modifiée : 6 mars 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur

- Heure modifiée : 18 mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La stratégie par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
"Sid" : "id2",
"Effect" : "Allow",
"Action" : [
  "dms:StartReplicationTask",
  "dms:StopReplicationTask",
  "dms>DeleteReplicationTask",
  "dms>DeleteReplicationInstance"
],
"Resource" : [
  "arn:aws:dms:*:*:rep:*",
  "arn:aws:dms:*:*:task:*"
],
"Condition" : {
  "StringEqualsIgnoreCase" : {
    "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
  }
}
},
{
  "Sid" : "id3",
  "Effect" : "Allow",
  "Action" : [
    "dms:TestConnection",
    "dms>DeleteConnection"
  ],
  "Resource" : [
    "arn:aws:dms:*:*:rep:*",
    "arn:aws:dms:*:*:endpoint:*"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy est une [politique AWS gérée](#) qui : Permet au service EC2 CapacityReservation Fleet de gérer les réservations de capacité

Utilisation des stratégies des politiques des politiques

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des stratégies des stratégies des stratégies des stratégies des stratégies des stratégies à

politiques des politiques des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 29 septembre 2021, 14:43 UTC
- Heure modifiée : 29 septembre 2021, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les stratégies qui définissent les stratégies qui permettent à d'effectuer les stratégies des stratégies qui sont des stratégies qui permettent à d'effectuer les stratégies. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document des stratégies JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateCapacityReservation",
      "ec2:CancelCapacityReservation",
      "ec2:ModifyCapacityReservation"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:capacity-reservation/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:capacity-reservation/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateCapacityReservation"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies gérées et évoluez vers les stratégies AWS gérées et évoluez vers les stratégies gérées et évoluez vers les stratégies gérées](#)

AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à EC2 Fleet de lancer et de gérer des instances.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 mars 2018, 00:08 UTC
- Heure modifiée : 4 mai 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSEC2SpotFleetServiceRolePolicy

AWSEC2SpotFleetServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à EC2 Spot Fleet de lancer et de gérer des instances de flotte d'instances Spot

Utilisation des politiques I

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 octobre 2017, 19:13 UTC
- Heure modifiée : 16 mars 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
  ],
}
```

```
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "ec2.amazonaws.com",
      "ec2.amazonaws.com.cn"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:spot-instances-request/*",
    "arn:aws:ec2:*:*:spot-fleet-request/*",
    "arn:aws:ec2:*:*:volume*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
```

```
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:*/*"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS et évoluez vers les autorisations de moindre privilège](#)

AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy est une [politiqueAWS gérée](#) qui : Permet à EC2 Spot de lancer et de gérer des instances ponctuelles

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 18 septembre 2017, 18:51 UTC
- Heure modifiée : 12 décembre 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec](#)

AWSECRPullThroughCache_ServiceRolePolicy

AWSECRPullThroughCache_ServiceRolePolicy est une [politique AWS gérée](#) qui : permet l'accès aux AWS services et aux ressources utilisés ou gérés par le AWS cache d'extraction ECR

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 26 novembre 2021, 21:51 UTC
- Heure modifiée : 13 novembre 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Sid" : "SecretsManager",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

AWSElasticBeanstalkCustomPlatformforEC2Role est une [politique AWS gérée](#) qui : accordez à l'instance dans votre environnement de création de plateforme personnalisé l'autorisation de lancer une instance EC2, de créer un instantané EBS et une AMI, de diffuser des journaux vers Amazon CloudWatch Logs et de stocker des artefacts dans Amazon S3.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkCustomPlatformforEC2Role les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 février 2017, 22:50 UTC
- Heure modifiée : 21 février 2017, 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2>DeleteKeypair",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteSnapshot",
        "ec2>DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
```

```

    "ec2:ModifySnapshotAttribute",
    "ec2:RegisterImage",
    "ec2:RunInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "BucketAccess",
  "Action" : [
    "s3:Get*",
    "s3:List*",
    "s3:PutObject"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkEnhancedHealth

AWSElasticBeanstalkEnhancedHealth est une [politique AWS gérée](#) qui : [Politique AWS Elastic Beanstalk Service](#) pour le système de surveillance de l'Health

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkEnhancedHealth les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 8 février 2016, 23:17 UTC
- Heure modifiée : 9 avril 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```

    "ec2:GetConsoleOutput",
    "ec2:AssociateAddress",
    "ec2:DescribeAddresses",
    "ec2:DescribeSecurityGroups",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeNotificationConfigurations",
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkMaintenance

AWSElasticBeanstalkMaintenance est une [politique AWS gérée](#) qui : La politique AWS Elastic Beanstalk Service Role accorde des autorisations limitées pour mettre à jour vos ressources en votre nom à des fins de maintenance.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 11 janvier 2019, 23:22 UTC
- Heure modifiée : 4 juin 2019, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  }
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy est une [politiqueAWS gérée](#) qui : Cette politique concerne le rôle de serviceAWS Elastic Beanstalk utilisé pour effectuer des mises à jour gérées des environnements Elastic Beanstalk. Cette politique ne doit pas être associée à d'autres utilisateurs ou rôles. La politique accorde des autorisations étendues pour créer et gérer des ressources sur un certain nombre deAWS services AutoScaling, notamment EC2, ECS, Elastic Load Balancing et CloudFormation. Cette politique permet également de transmettre tout rôle IAM utilisable avec ces services.

Utilisation de cette stratégie

Vous pouvezAWSElasticBeanstalkManagedUpdatesCustomerRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 mars 2021, 22:18 UTC
- Heure modifiée : 23 mars 2023, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "autoscaling:DescribeAccountLimits",
  "autoscaling:DescribeAutoScalingGroups",
  "autoscaling:DescribeAutoScalingInstances",
  "autoscaling:DescribeLaunchConfigurations",
  "autoscaling:DescribeLoadBalancers",
  "autoscaling:DescribeNotificationConfigurations",
  "autoscaling:DescribeScalingActivities",
  "autoscaling:DescribeScheduledActions",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAddresses",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeImages",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstances",
  "ec2:DescribeKeyPairs",
  "ec2:DescribeLaunchTemplates",
  "ec2:DescribeLaunchTemplateVersions",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSnapshots",
  "ec2:DescribeSpotInstanceRequests",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcClassicLink",
  "ec2:DescribeVpcs",
  "elasticloadbalancing:DescribeInstanceHealth",
  "elasticloadbalancing:DescribeLoadBalancers",
  "elasticloadbalancing:DescribeTargetGroups",
  "elasticloadbalancing:DescribeTargetHealth",
  "logs:DescribeLogGroups",
  "rds:DescribeDBEngineVersions",
  "rds:DescribeDBInstances",
  "rds:DescribeOrderableDBInstanceOptions",
  "sns:ListSubscriptionsByTopic"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "EC2BroadOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
```

```

    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions",
    "ec2>DeleteSecurityGroup",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2RunInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "EC2TerminateInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  }
},
{
  "Sid" : "ECSBroadOperationPermissions",

```

```

    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs:DescribeClusters",
      "ecs:RegisterTaskDefinition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ECSDeleteClusterOperationPermissions",
    "Effect" : "Allow",
    "Action" : "ecs:DeleteCluster",
    "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
  },
  {
    "Sid" : "ASGOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DetachInstances",
      "autoscaling>DeletePolicy",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:ResumeProcesses",
      "autoscaling:SetDesiredCapacity",
      "autoscaling:SuspendProcesses",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource" : [
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
    ]
  },
},

```

```

{
  "Sid" : "CFNOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:*"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "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"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy est une [politique AWS gérée](#) qui : [politique AWS Elastic Beanstalk Service Role](#) qui accorde des autorisations limitées pour les mises à jour gérées.

utilisation une une une des politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les des des des des des des des rôles.

les les les les

- Type : Politique de rôles liée à un service
- Heure de création : 21 novembre 2019, 22:35 UTC
- Heure modifiée : 24 mars 2023, 00:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Version de la politique

Version de la politique :v8 (par défaut)

La de stratégie est la version qui est la version qui est la version qui définit les des politiques qui est la version qui définit les des politiques qui Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

un document de de

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



```
"Condition" : {
  "StringLikeIfExists" : {
    "iam:PassedToService" : [
      "elasticbeanstalk.amazonaws.com",
      "ec2.amazonaws.com",
      "autoscaling.amazonaws.com",
      "elasticloadbalancing.amazonaws.com",
      "ecs.amazonaws.com",
      "cloudformation.amazonaws.com"
    ]
  }
},
{
  "Sid" : "SingleInstanceAPIs",
  "Effect" : "Allow",
  "Action" : [
    "ec2:releaseAddress",
    "ec2:allocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ECS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:RegisterTaskDefinition",
    "ecs:DeRegisterTaskDefinition",
    "ecs:List*",
    "ecs:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ElasticBeanstalkAPIs",
  "Effect" : "Allow",
  "Action" : [
    "elasticbeanstalk:*"
  ],
  "Resource" : "*"
},
{
```

```

    "Sid" : "ReadOnlyAPIs",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ASG",
    "Effect" : "Allow",
    "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling>DeleteAutoScalingGroup",
        "autoscaling>DeleteLaunchConfiguration",
        "autoscaling>DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
    ]
},

```

```
{
  "Sid" : "CFN",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CancelUpdateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation:UpdateStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-e-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  }
},
{
  "Sid" : "S3Obj",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl"
  ],
}
```

```

    "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
  },
  {
    "Sid" : "S3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy",
      "s3:ListBucket",
      "s3:PutBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
  },
  {
    "Sid" : "CWL",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs>DeleteLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
  },
  {
    "Sid" : "ELB",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeRegisterTargets",
      "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
      "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
    ]
  },
  {
    "Sid" : "SNS",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic"
    ]
  }

```

```
    ],
    "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
  },
  {
    "Sid" : "EC2LaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate",
      "ec2>DeleteLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*"
  },
  {
    "Sid" : "AllowLaunchTemplateRunInstances",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "RegisterTaskDefinition"
        ]
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [des politiquesAWS gérées et évoluez avec les des des des des des des des des des des des des de de de](#)

AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDockerest une [politiqueAWS gérée](#) qui : accordez aux instances de votre environnement Docker multiconteneur un accès pour utiliser Amazon EC2 Container Service afin de gérer les tâches de déploiement de conteneurs.

Utilisation de cette stratégie

Vous pouvezAWSElasticBeanstalkMulticontainerDocker les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 février 2016, 23:15 UTC
- Heure modifiée : 23 mars 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Sid" : "ECSAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:Poll",
    "ecs:StartTask",
    "ecs:StopTask",
    "ecs:DiscoverPollEndpoint",
    "ecs:StartTelemetrySession",
    "ecs:RegisterContainerInstance",
    "ecs:DeregisterContainerInstance",
    "ecs:DescribeContainerInstances",
    "ecs:Submit*",
    "ecs:DescribeTasks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "RegisterContainerInstance",
        "StartTask"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly est une [politique AWS gérée](#) qui : accorde des autorisations en lecture seule. Permet explicitement aux opérateurs d'accéder directement aux informations relatives aux ressources liées aux applications AWS Elastic Beanstalk.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 22 janvier 2021, 19:02 UTC
- Heure modifiée : 22 janvier 2021, 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
```



```
"autoscaling:DescribeLoadBalancers",
"autoscaling:DescribeNotificationConfigurations",
"autoscaling:DescribeScalingActivities",
"autoscaling:DescribeScheduledActions",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"cloudformation:GetTemplate",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ValidateTemplate",
"cloudtrail:LookupEvents",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplateVersions",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSSLPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"iam:GetRole",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListRolePolicies",
```

```
    "iam:ListRoles",
    "iam:ListServerCertificates",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribeDBSnapshots",
    "s3:ListAllMyBuckets",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowS3",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore est une [politique AWS gérée](#) qui : AWSElasticBeanstalkRoleCore (rôle opérationnel d'Elastic Beanstalk) Autorise le fonctionnement de base d'un environnement de services Web.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkRoleCore les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2020, 21:48 UTC
- Heure modifiée : 09 septembre 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```

        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
    }
}
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReleaseAddress",
    "ec2:AllocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteSecurityGroup",
    "ec2:AuthorizeSecurityGroup*",
    "ec2:RevokeSecurityGroup*",
    "ec2:CreateLaunchTemplate*",
    "ec2>DeleteLaunchTemplate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LTRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:*LoadBalancer*",
    "autoscaling:*AutoScalingGroup",
    "autoscaling:*LaunchConfiguration",
    "autoscaling>DeleteScheduledAction",

```

```

        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
    ],
    "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
    ]
},
{
    "Sid" : "ASGPolicy",
    "Effect" : "Allow",
    "Action" : [
        "autoscaling:DeletePolicy"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "EBSLR",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
    ],
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
    }
},
{
    "Sid" : "S30bj",
    "Effect" : "Allow",
    "Action" : [

```

```

    "s3:Delete*",
    "s3:Get*",
    "s3:Put*"
  ],
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*/**",
    "arn:aws:s3:::elasticbeanstalk-env-resources-*/**"
  ]
},
{
  "Sid" : "S3Bucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucket*",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Sid" : "CFN",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation:ListStackResources",
    "cloudformation:UpdateStack",
    "cloudformation:ContinueUpdateRollback",
    "cloudformation:CancelUpdateStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
},
{
  "Sid" : "ELB",

```

```

"Effect" : "Allow",
"Action" : [
  "elasticloadbalancing:Create*",
  "elasticloadbalancing>Delete*",
  "elasticloadbalancing:Modify*",
  "elasticloadbalancing:RegisterTargets",
  "elasticloadbalancing:DeRegisterTargets",
  "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
  "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
  "elasticloadbalancing:*Tags",
  "elasticloadbalancing:ConfigureHealthCheck",
  "elasticloadbalancing:SetRulePriorities",
  "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
],
"Resource" : [
  "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
  "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
  "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/**",
  "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/**",
  "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
  "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
  "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
  "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/**/**/*"
]
},
{
  "Sid" : "ListAPIs",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*",
    "cloudformation:Describe*",
    "logs:Describe*",
    "ec2:Describe*",
    "ecs:Describe*",
    "ecs:List*",
    "elasticloadbalancing:Describe*",
    "rds:Describe*",
    "sns:List*",
    "iam:List*",
    "acm:Describe*",
    "acm:List*"
  ],
  "Resource" : "*"
},

```

```
{
  "Sid" : "AllowPassRole",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "elasticbeanstalk.amazonaws.com",
        "ec2.amazonaws.com",
        "autoscaling.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "ecs.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleCWL

AWSElasticBeanstalkRoleCWL est une [politique AWS gérée](#) qui : (rôle opérationnel d'Elastic Beanstalk) Autorise un environnement à gérer les groupes de CloudWatch journaux Amazon Logs.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkRoleCWL les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 5 juin 2020, 21:49 UTC
- Heure modifiée : 5 juin 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS est une [politique AWS gérée](#) qui : (rôle opérationnel d'Elastic Beanstalk) Permet à un environnement Docker multiconteneur de gérer des clusters Amazon ECS.

Utilisation de cette stratégie

Vous pouvez les associer AWSElasticBeanstalkRoleECS à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2020, 21:47 UTC
- Heure modifiée : 23 mars 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs>DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "CreateCluster",
          "RegisterTaskDefinition"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleRDS

AWSElasticBeanstalkRoleRDS est une [politique AWS gérée](#) qui : (rôle opérationnel d'Elastic Beanstalk) Autorise un environnement à intégrer une instance Amazon RDS.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkRoleRDS les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2020, 21:46 UTC
- Heure modifiée : 5 juin 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds>DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds>DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS est une [politiqueAWS gérée](#) qui : (rôle opérationnel d'Elastic Beanstalk) Autorise un environnement à activer l'intégration des rubriques Amazon SNS.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkRoleSNS les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2020, 21:46 UTC
- Heure modifiée : 5 juin 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Sid" : "AllowBeanstalkManageSNS",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:SetTopicAttributes",
      "sns>DeleteTopic"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    ]
  },
  {
    "Sid" : "AllowSNSPublish",
    "Effect" : "Allow",
    "Action" : [
      "sns:GetTopicAttributes",
      "sns:Subscribe",
      "sns:Unsubscribe",
      "sns:Publish"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkRoleWorkerTier

AWSElasticBeanstalkRoleWorkerTier est une [politique AWS gérée](#) qui : (rôle opérationnel Elastic Beanstalk) Permet à un niveau d'environnement de travail de créer une table Amazon DynamoDB et une file d'attente Amazon SQS.

Utilisation de cette stratégie

Vous pouvez les associer `AWSElasticBeanstalkRoleWorkerTier` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2020, 21:43 UTC
- Heure modifiée : 5 juin 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs>DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs>CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
```

```
"Effect" : "Allow",
"Action" : [
  "dynamodb:CreateTable",
  "dynamodb:TagResource",
  "dynamodb:DescribeTable",
  "dynamodb>DeleteTable"
],
"Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkService

AWSElasticBeanstalkService est une [politique AWS gérée](#) qui : Cette politique est en voie d'obsolescence. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Politique de rôles d'Elastic Beanstalk Service qui accorde les autorisations nécessaires pour créer et gérer des ressources (par exemple AutoScaling, EC2CloudFormation, S3, ELB, etc.) en votre nom.

Utilisation de cette stratégie

Vous pouvez AWSElasticBeanstalkService les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 avril 2016, 20:27 UTC
- Heure modifiée : 10 mai 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Version de la politique

Version de la politique :v17 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
        ]
    }
},
{
    "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
    "Effect" : "Allow",
    "Action" : [
        "s3:*"
    ],
    "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
    ]
},
{
    "Sid" : "AllowLaunchTemplateRunInstances",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
        "ArnLike" : {
            "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
    }
},
{
    "Sid" : "AllowELBAddTags",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "elasticloadbalancing:CreateAction" : [
                "CreateLoadBalancer"
            ]
        }
    }
},
},
```

```
{
  "Sid" : "AllowOperations",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteScheduledAction",
    "autoscaling:DescribeAccountLimits",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLoadBalancers",
    "autoscaling:DescribeNotificationConfigurations",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeScheduledActions",
    "autoscaling:DetachInstances",
    "autoscaling>DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:ResumeProcesses",
    "autoscaling:SetDesiredCapacity",
    "autoscaling:SuspendProcesses",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup",
    "cloudwatch:PutMetricAlarm",
    "ec2:AssociateAddress",
    "ec2:AllocateAddress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
```

```
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeVpcClassicLink",
"ec2:DisassociateAddress",
"ec2:ReleaseAddress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:TerminateInstances",
"ecs:CreateCluster",
"ecs>DeleteCluster",
"ecs:DescribeClusters",
"ecs:RegisterTaskDefinition",
"elasticbeanstalk:*",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing>DeleteLoadBalancer",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:DeregisterTargets",
"iam:ListRoles",
"iam:PassRole",
"logs:CreateLogGroup",
"logs:PutRetentionPolicy",
"logs:DescribeLogGroups",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeOrderableDBInstanceOptions",
"s3:GetObject",
"s3:GetObjectAcl",
"s3:ListBucket",
"sns:CreateTopic",
```

```
    "sns:GetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "sns:Subscribe",
    "sns:SetTopicAttributes",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkServiceRolePolicy

AWSElasticBeanstalkServiceRolePolicy est une [politiqueAWS gérée](#) qui : la politiqueAWS Elastic Beanstalk Service Linked Role accorde des autorisations pour créer et gérer des ressources (c'est-à-dire : AutoScaling EC2 CloudFormation, S3, ELB, etc.) en votre nom.

Utilisation des des des des des des

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des rôles des rôles des utilisateurs des politiques gérées des politiques gérées des

Les des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 septembre 2017, 23:46 UTC
- Heure modifiée : 6 juin 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version par défaut des politiques, qui définit des stratégies gérées par défaut des politiques gérées par la stratégie stratégie stratégie qui définit des Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document des politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
```

```

    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeNotificationConfigurations",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:PutNotificationConfiguration",
    "ec2:DescribeInstanceStatus",
    "ec2:AssociateAddress",
    "ec2:DescribeAddresses",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeTargetGroups",
    "lambda:GetFunction",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowOperationsOnHealthStreamingLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs>DeleteLogGroup",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des politiques AWS gérées gérées gérées gérées gérées gérées gérées gérées et évoluez vers des autorisations gérées des stratégies gérées gérées gérées gérées gérées gérées gérées gérées](#)

AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier est une [politique AWS gérée](#) qui : permet aux instances de votre environnement de serveur Web d'accéder à des fichiers journaux vers Amazon S3.

Utilisation de cette stratégie

Vous pouvez les associer AWSElasticBeanstalkWebTier à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 février 2016, 23:08 UTC
- Heure modifiée : 09 septembre 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
```



```
    "arn:aws:s3:::elasticbeanstalk-*/**"
  ],
},
{
  "Sid" : "XRayAccess",
  "Action" : [
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetSamplingStatisticSummaries"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:PutLogEvents",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
  ]
},
{
  "Sid" : "ElasticBeanstalkHealthAccess",
  "Action" : [
    "elasticbeanstalk:PutInstanceStatistics"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:elasticbeanstalk:*:*:application/*",
    "arn:aws:elasticbeanstalk:*:*:environment/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTierest une [politiqueAWS gérée](#) qui : permet aux instances de votre environnement de travail d'accéder à des fichiers journaux vers Amazon S3, d'utiliser Amazon SQS pour surveiller la file d'attente des tâches de votre candidature, d'utiliser Amazon DynamoDB pour procéder à l'élection des leaders et à Amazon CloudWatch pour publier des statistiques à des fins de surveillance de l'état de santé.

Utilisation de cette stratégie

Vous pouvezAWSElasticBeanstalkWorkerTier les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 février 2016, 23:12 UTC
- Heure modifiée : 09 septembre 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "MetricsAccess",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "XRayAccess",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingRules",
      "xray:GetSamplingTargets",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "QueueAccess",
    "Action" : [
      "sqs:ChangeMessageVisibility",
      "sqs:DeleteMessage",
      "sqs:ReceiveMessage",
      "sqs:SendMessage"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "BucketAccess",
    "Action" : [
      "s3:Get*",
      "s3:List*",
      "s3:PutObject"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:s3:::elasticbeanstalk-*",
      "arn:aws:s3:::elasticbeanstalk-*/*"
    ]
  }
]
```

```
]
},
{
  "Sid" : "DynamoPeriodicTasks",
  "Action" : [
    "dynamodb:BatchGetItem",
    "dynamodb:BatchWriteItem",
    "dynamodb:DeleteItem",
    "dynamodb:GetItem",
    "dynamodb:PutItem",
    "dynamodb:Query",
    "dynamodb:Scan",
    "dynamodb:UpdateItem"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
  ]
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:PutLogEvents",
    "logs:CreateLogStream"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
  ]
},
{
  "Sid" : "ElasticBeanstalkHealthAccess",
  "Action" : [
    "elasticbeanstalk:PutInstanceStatistics"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:elasticbeanstalk:*:*:application/*",
    "arn:aws:elasticbeanstalk:*:*:environment/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

AWSElasticDisasterRecoveryAgentInstallationPolicy est une [politique AWS gérée](#) qui : Cette politique permet d'installer l'agent de AWS réplication, qui est utilisé avec AWS Elastic Disaster Recovery (DRS) pour restaurer des serveurs externes sur AWS. Associez cette politique aux utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'étape d'installation de l'agent de AWS réplication.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryAgentInstallationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:37 UTC
- Heure modifiée : 27 novembre 2023, 12h38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
```

```
"Effect" : "Allow",
"Action" : "drs:TagResource",
"Resource" : "arn:aws:drs:*:*:source-network/*",
"Condition" : {
  "StringEquals" : {
    "drs:CreateAction" : "CreateSourceNetwork"
  }
},
{
  "Sid" : "DRSAgentInstallationPolicy5",
  "Effect" : "Allow",
  "Action" : "drs:IssueAgentCertificateForDrs",
  "Resource" : "arn:aws:drs:*:*:source-server/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryAgentPolicy

AWSElasticDisasterRecoveryAgentPolicy est une [politique AWS gérée](#) qui : Cette politique permet d'utiliser l'agent de AWS réplication, qui est utilisé avec AWS Elastic Disaster Recovery (DRS) pour restaurer les serveurs sources sur AWS. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 17 novembre 2021, 10:32 UTC
- Heure modifiée : 27 novembre 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
  ],
}
```



```
    "Sid" : "DRSAgentPolicy2",
    "Effect" : "Allow",
    "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryConsoleFullAccess

AWSElasticDisasterRecoveryConsoleFullAccess est une [politique AWS gérée](#) qui : Cette [politique](#) fournit un accès complet à toutes les API publiques d'AWSElastic Disaster Recovery (DRS), ainsi que des autorisations pour lire les informations relatives aux clés KMS, au License Manager, aux Resource Groups, à Elastic Load Balancing, à IAM et à EC2. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:46 UTC
- Heure modifiée : 16 octobre 2023, 12h24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess4",
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess5",
  "Effect" : "Allow",
  "Action" : "resource-groups:ListGroups",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess6",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess7",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess8",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
```

```
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
    ],
    "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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

AWSElasticDisasterRecoveryConsoleFullAccess_v2 est une [politique AWS gérée](#) qui : Cette politique fournit un accès complet à toutes les API publiques d'AWSElastic Disaster Recovery (AWSDRS), ainsi qu'à toutes les API publiques AWS des autres services utilisés par la console AWS DRS. Associez cette politique à vos utilisateurs ou à vos rôles.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryConsoleFullAccess_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2023, 13:35 UTC
- Heure modifiée : 27 novembre 2023, 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
```

```
"Action" : [
  "drs:*"
],
"Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess2",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess4",
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups:ListGroup",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess6",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess7",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess8",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess9",
    "Effect" : "Allow",
```

```
"Action" : [
  "ec2:DeleteSnapshot"
],
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
}
},
{
  "Sid" : "ConsoleFullAccess10",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions",
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
```

```
"Sid" : "ConsoleFullAccess12",
"Effect" : "Allow",
"Action" : [
  "ec2:DeleteVolume"
],
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
}
},
{
  "Sid" : "ConsoleFullAccess13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
},
{
  "Sid" : "ConsoleFullAccess14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
}
```



```
"Resource" : "arn:aws:ec2:*:*:security-group/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess15",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess16",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "ConsoleFullAccess17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
```

```
        "aws:ViaAWSService" : "true"
    }
}
},
{
  "Sid" : "ConsoleFullAccess18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess19",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess20",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
"Condition" : {
  "Null" : {
    "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess21",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume",
    "ec2:StartInstances",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ConsoleFullAccess22",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "ConsoleFullAccess23",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess24",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess25",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
```

```
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess26",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess27",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate"
      ]
    }
  }
}
```

```
  },
  {
    "Sid" : "ConsoleFullAccess28",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess29",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess30",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation"
    ],
    "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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryConversionServerPolicy

AWSElasticDisasterRecoveryConversionServerPolicy est une [politique AWS gérée](#) qui : Cette politique est attachée au rôle d'instance du serveur AWS Elastic Disaster Recovery Conversion. Cette politique permet aux serveurs de conversion Elastic Disaster Recovery (DRS), qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS. Un rôle IAM conforme à cette politique est attaché (sous forme de profil d'instance EC2) par DRS aux serveurs de conversion DRS, qui sont automatiquement lancés et interrompus par DRS en cas de besoin. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM. Les serveurs de conversion DRS sont utilisés par Elastic Disaster Recovery lorsque les utilisateurs choisissent de restaurer les serveurs sources à l'aide de la console, de la CLI ou de l'API DRS.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryConversionServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 17 novembre 2021, 13:42 UTC
- Heure modifiée : 27 novembre 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy est une [politique AWS gérée](#) qui : [Cette politique](#) permet à AWS Elastic Disaster Recovery (DRS) de prendre en charge la réplication entre comptes et le repli entre comptes.

Utilisation de cette politique

Vous pouvez vous associer

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 14 mai 2023, 07:16 UTC
- Heure modifiée : 17 janvier 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

AWSElasticDisasterRecoveryEc2InstancePolicy est une [politique AWS gérée](#) qui : Cette politique permet d'installer et d'utiliser l'agent de AWS réplication, qui est utilisé par AWS Elastic Disaster Recovery (DRS) pour récupérer les serveurs sources qui s'exécutent sur EC2 (inter-régions ou cross-AZ). Un rôle IAM conforme à cette politique doit être attaché (sous forme de profil d'instance EC2) aux instances EC2.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryEc2InstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 mai 2022, 12h30 UTC
- Heure modifiée : 27 novembre 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
```

```

        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DRSEc2InstancePolicy2",
    "Effect" : "Allow",
    "Action" : [
        "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
        "StringEquals" : {
            "drs:CreateAction" : "CreateSourceServerForDrs"
        }
    }
},
{
    "Sid" : "DRSEc2InstancePolicy3",
    "Effect" : "Allow",
    "Action" : [
        "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-network/*",
    "Condition" : {
        "StringEquals" : {
            "drs:CreateAction" : "CreateSourceNetwork"
        }
    }
},
{
    "Sid" : "DRSEc2InstancePolicy4",
    "Effect" : "Allow",
    "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",

```

```

        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*"
},
{
    "Sid" : "DRSEc2InstancePolicy5",
    "Effect" : "Allow",
    "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
            "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

AWSElasticDisasterRecoveryFailbackInstallationPolicy est une [politique AWS gérée](#) qui : Vous pouvez associer la AWSElasticDisasterRecoveryFailbackInstallationPolicy politique à vos identités IAM. Cette politique permet d'installer le client Elastic Disaster Recovery Failback, qui est

utilisé pour rétablir les instances de restauration dans votre infrastructure source d'origine. Associez cette politique aux utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'exécution du client Elastic Disaster Recovery Failback.

Utilisation de cette politique

Vous pouvez vous associer `AWSElasticDisasterRecoveryFailbackInstallationPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 11:02 UTC
- Heure modifiée : 27 novembre 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryFailbackPolicy

AWSElasticDisasterRecoveryFailbackPolicy est une [politique AWS gérée](#) qui : Cette politique permet d'utiliser le client Elastic Disaster Recovery Failback, qui est utilisé pour rétablir les instances de restauration dans votre infrastructure source d'origine. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryFailbackPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service

- Heure de création : 17 novembre 2021, 10:41 UTC
- Heure modifiée : 27 novembre 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
```

```

    "drs:DescribeReplicationServerAssociationsForDrs",
    "drs:DescribeRecoveryInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSFailbackPolicy4",
  "Effect" : "Allow",
  "Action" : [
    "drs:GetFailbackCommandForDrs",
    "drs:UpdateFailbackClientLastSeenForDrs",
    "drs:NotifyAgentAuthenticationForDrs",
    "drs:UpdateAgentReplicationProcessStateForDrs",
    "drs:NotifyAgentReplicationProgressForDrs",
    "drs:NotifyAgentConnectedForDrs",
    "drs:NotifyAgentDisconnectedForDrs",
    "drs:NotifyConsistencyAttainedForDrs",
    "drs:GetFailbackLaunchRequestedForDrs",
    "drs:IssueAgentCertificateForDrs"
  ],
  "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

AWSElasticDisasterRecoveryLaunchActionsPolicy est une [politique AWS gérée](#) qui : Cette politique vous permet d'utiliser les autorisations requises par Amazon SSM et les services supplémentaires pour exécuter des actions après le lancement dans AWS Elastic Disaster Recovery (AWSDRS). Associez cette politique à vos rôles ou utilisateurs IAM.

Utilisation de cette politique

Vous pouvez vous associer `AWSElasticDisasterRecoveryLaunchActionsPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 septembre 2023, 07:38 UTC
- Heure modifiée : 16 octobre 2023, 12h28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Sid" : "LaunchActionsPolicy2",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/*",
    "arn:aws:ssm:*:*:automation-definition/*:*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    },
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "LaunchActionsPolicy3",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-*",
    "arn:aws:ssm:*:*:document/AWSCodeDeployAgent-*",
    "arn:aws:ssm:*:*:document/AWSConfigRemediation-*",
    "arn:aws:ssm:*:*:document/AWSConformancePacks-*",
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-*",
    "arn:aws:ssm:*:*:document/AWSDistro0Tel-*",
    "arn:aws:ssm:*:*:document/AWSDocs-*",
    "arn:aws:ssm:*:*:document/AWSEC2-*",
    "arn:aws:ssm:*:*:document/AWSEC2Launch-*",
    "arn:aws:ssm:*:*:document/AWSFIS-*",
    "arn:aws:ssm:*:*:document/AWSFleetManager-*",

```

```
"arn:aws:ssm:*::document/AWSIncidents-*",
"arn:aws:ssm:*::document/AWSKinesisTap-*",
"arn:aws:ssm:*::document/AWSMigration-*",
"arn:aws:ssm:*::document/AWSNVMe-*",
"arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
"arn:aws:ssm:*::document/AWSObservabilityExporter-*",
"arn:aws:ssm:*::document/AWSPVDriver-*",
"arn:aws:ssm:*::document/AWSQuickSetupType-*",
"arn:aws:ssm:*::document/AWSQuickStarts-*",
"arn:aws:ssm:*::document/AWSRefactorSpaces-*",
"arn:aws:ssm:*::document/AWSResilienceHub-*",
"arn:aws:ssm:*::document/AWSSAP-*",
"arn:aws:ssm:*::document/AWSSAPTools-*",
"arn:aws:ssm:*::document/AWSSQLServer-*",
"arn:aws:ssm:*::document/AWSSSO-*",
"arn:aws:ssm:*::document/AWSSupport-*",
"arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
"arn:aws:ssm:*::document/AmazonCloudWatch-*",
"arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
"arn:aws:ssm:*::document/AmazonECS-*",
"arn:aws:ssm:*::document/AmazonEFSUtils-*",
"arn:aws:ssm:*::document/AmazonEKS-*",
"arn:aws:ssm:*::document/AmazonInspector-*",
"arn:aws:ssm:*::document/AmazonInspector2-*",
"arn:aws:ssm:*::document/AmazonInternal-*",
"arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
"arn:aws:ssm:*::document/AwsVssComponents-*",
"arn:aws:ssm:*::automation-definition/AWS-*:*",
"arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
"arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
"arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
"arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
"arn:aws:ssm:*::automation-definition/AWSDistro0Tel-*:*",
"arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
"arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
"arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
"arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
"arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
"arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
"arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
"arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
"arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
"arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
"arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
```

```

    "arn:aws:ssm::*:automation-definition/AWSPVDriver-*:*",
    "arn:aws:ssm::*:automation-definition/AWSQuickSetupType-*:*",
    "arn:aws:ssm::*:automation-definition/AWSQuickStarts-*:*",
    "arn:aws:ssm::*:automation-definition/AWSRefactorSpaces-*:*",
    "arn:aws:ssm::*:automation-definition/AWSResilienceHub-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSAP-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSAPTools-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSQLServer-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSSO-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSupport-*:*",
    "arn:aws:ssm::*:automation-definition/AWSSystemsManagerSAP-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonCloudWatch-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonCloudWatchAgent-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonECS-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonEFSUtils-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonEKS-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInspector-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInspector2-*:*",
    "arn:aws:ssm::*:automation-definition/AmazonInternal-*:*",
    "arn:aws:ssm::*:automation-definition/AwsEnaNetworkDriver-*:*",
    "arn:aws:ssm::*:automation-definition/AwsVssComponents-*:*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "LaunchActionsPolicy4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2::*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
}

```

```
    },
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  },
  {
    "Sid" : "LaunchActionsPolicy5",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy6",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListDocuments",
      "ssm:ListCommandInvocations"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LaunchActionsPolicy7",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListDocumentVersions",
      "ssm:GetDocument",
      "ssm:DescribeDocument"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/*"
```



```
  },
  {
    "Sid" : "LaunchActionsPolicy8",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy9",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecoveryService-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "LaunchActionsPolicy10",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter",
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecoveryService-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
```

```

    "Sid" : "LaunchActionsPolicy11",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "drs.amazonaws.com"
      }
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

AWSElasticDisasterRecoveryNetworkReplicationPolicy est une [politique AWS gérée qui](#) : [Cette politique](#) permet à AWS Elastic Disaster Recovery (DRS) de prendre en charge la réplication réseau.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryNetworkReplicationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service

- Heure de création : 11 juin 2023, 12:36 UTC
- Heure modifiée : 2 janvier 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS ElasticDisasterRecoveryNetworkReplicationPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryReadOnlyAccess

AWSElasticDisasterRecoveryReadOnlyAccess est une [politique AWS gérée](#) qui : Vous pouvez associer la AWSElasticDisasterRecoveryReadOnlyAccess politique à vos identités IAM. Cette politique fournit des autorisations à toutes les API publiques en lecture seule d'Elastic Disaster Recovery (DRS), ainsi qu'à certaines API en lecture seule d'autres AWS services nécessaires pour utiliser pleinement la console DRS en lecture seule. Associez cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:50 UTC
- Heure modifiée : 27 novembre 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    }
  ],
  {
```

```

    "Sid" : "DRSReadOnlyAccess5",
    "Effect" : "Allow",
    "Action" : "ssm:ListCommandInvocations",
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReadOnlyAccess6",
    "Effect" : "Allow",
    "Action" : "ssm:GetParameter",
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
  },
  {
    "Sid" : "DRSReadOnlyAccess7",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWS-CreateImage",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
      "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
      "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
    ]
  },
  {
    "Sid" : "DRSReadOnlyAccess8",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
]

```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

AWSElasticDisasterRecoveryRecoveryInstancePolicy est une [politique AWS gérée](#) qui : Cette politique est attachée au rôle d'instance de l'instance de restauration d'Elastic Disaster Recovery. Cette politique permet aux instances de restauration Elastic Disaster Recovery (DRS), qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS et de revenir à leur infrastructure source d'origine. Un rôle IAM conforme à cette politique est attaché (sous forme de profil d'instance EC2) par Elastic Disaster Recovery aux instances de restauration DRS. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryRecoveryInstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 17 novembre 2021, 10:20 UTC
- Heure modifiée : 27 novembre 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
```



```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceTypes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy4",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetAgentInstallationAssetsForDrs",
      "drs:SendClientLogsForDrs",
      "drs:CreateSourceServerForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy5",
    "Effect" : "Allow",
    "Action" : [
      "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceServerForDrs"
      }
    }
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy6",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendAgentMetricsForDrs",
      "drs:SendAgentLogsForDrs",
      "drs:UpdateAgentSourcePropertiesForDrs",
      "drs:UpdateAgentReplicationInfoForDrs",
      "drs:UpdateAgentConversionInfoForDrs",
      "drs:GetAgentCommandForDrs",
      "drs:GetAgentConfirmedResumeInfoForDrs",
      "drs:GetAgentRuntimeConfigurationForDrs",
      "drs:UpdateAgentBacklogForDrs",
      "drs:GetAgentReplicationInfoForDrs"
    ],
  },

```

```

    "Resource" : "arn:aws:dms:*:*: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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

AWSElasticDisasterRecoveryReplicationServerPolicy est une [politique AWS gérée](#) qui : Cette politique est attachée au rôle d'instance du serveur Elastic Disaster Recovery Replication. Cette politique permet aux serveurs de réplication Elastic Disaster Recovery (DRS), qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS et de créer des instantanés EBS dans votre. Compte AWS Un rôle IAM conforme à cette politique est attaché (sous forme de profil d'instance EC2) par Elastic Disaster Recovery aux serveurs de

réplication DRS qui sont automatiquement lancés et arrêtés par DRS, selon les besoins. Les serveurs de réplication DRS sont utilisés pour faciliter la réplication des données depuis vos serveurs externes vers AWS, dans le cadre du processus de restauration géré par DRS. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer `AWSElasticDisasterRecoveryReplicationServerPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 17 novembre 2021, 13:34 UTC
- Heure modifiée : 27 novembre 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "DRSReplicationServerPolicy2",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetChannelCommandsForDrs",
      "drs:SendChannelCommandResultForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy3",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetAgentSnapshotCreditsForDrs",
      "drs:DescribeReplicationServerAssociationsForDrs",
      "drs:DescribeSnapshotRequestsForDrs",
      "drs:BatchDeleteSnapshotRequestForDrs",
      "drs:NotifyAgentAuthenticationForDrs",
      "drs:BatchCreateVolumeSnapshotGroupForDrs",
      "drs:UpdateAgentReplicationProcessStateForDrs",
      "drs:NotifyAgentReplicationProgressForDrs",
      "drs:NotifyAgentConnectedForDrs",
      "drs:NotifyAgentDisconnectedForDrs",
      "drs:NotifyVolumeEventForDrs",
      "drs:SendVolumeStatsForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy4",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy5",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
  },
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
},
{
  "Sid" : "DRSReplicationServerPolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSReplicationServerPolicy7",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateSnapshot"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryServiceRolePolicy

AWSElasticDisasterRecoveryServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique permet à Elastic Disaster Recovery de gérer les AWS ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 17 novembre 2021, 10:56 UTC
- Heure modifiée : 17 janvier 2024, 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Sid" : "DRSServiceRolePolicy2",
  "Effect" : "Allow",
  "Action" : [
    "drs:TagResource"
  ],
  "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
},
{
  "Sid" : "DRSServiceRolePolicy3",
  "Effect" : "Allow",
  "Action" : [
    "drs:CreateRecoveryInstanceForDrs",
    "drs:TagResource"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*"
},
{
  "Sid" : "DRSServiceRolePolicy4",
  "Effect" : "Allow",
  "Action" : "iam:GetInstanceProfile",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy5",
  "Effect" : "Allow",
  "Action" : "kms:ListRetirableGrants",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2: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" : "*"
  }
]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy est une [politique AWS gérée](#) qui : Cette politique autorise un accès en lecture seule aux ressources AWS Elastic Disaster Recovery (DRS) telles que les serveurs sources et les tâches. Il permet également de créer un instantané converti et de partager cet instantané EBS avec un compte spécifique.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryStagingAccountPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 mai 2022, 09:49 UTC
- Heure modifiée : 27 novembre 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 est une [politique AWS gérée](#) qui : Cette politique est utilisée par AWS Elastic Disaster Recovery (DRS) pour restaurer les serveurs sources sur un compte cible distinct et pour permettre le retour en panne. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSElasticDisasterRecoveryStagingAccountPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 05 janvier 2023, 12:11 UTC
- Heure modifiée : 27 novembre 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Sid" : "DRSStagingAccountPolicyv21",
    "Effect" : "Allow",
    "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DRSStagingAccountPolicyv22",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
            "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
    }
},
{
    "Sid" : "DRSStagingAccountPolicyv23",
    "Effect" : "Allow",
    "Action" : "drs:IssueAgentCertificateForDrs",
    "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

AWSElasticLoadBalancingClassicServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle liée aux services pour AWS Elastic Load Balancing Control Plane - Classic

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 septembre 2017, 22:36 UTC
- Heure modifiée : 7 octobre 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "ec2:DescribeAddresses",
    "ec2:DescribeInstances",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeClassicLinkInstances",
    "ec2:DescribeVpcClassicLink",
    "ec2:CreateSecurityGroup",
    "ec2:CreateNetworkInterface",
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:AttachNetworkInterface",
    "ec2:DetachNetworkInterface",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElasticLoadBalancingServiceRolePolicy

AWSElasticLoadBalancingServiceRolePolicy est une [politiqueAWS gérée qui : Politique](#) de rôle liée aux services pourAWS Elastic Load Balancing Control Plane

Utilisation cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

détails des politique

- Type : Politique de rôles liée à un service
- Heure de création : 19 septembre 2017, 22:19 UTC
- Heure modifiée : 26 août 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de politique est la version qui définit autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
"ec2:AllocateAddress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:AttachNetworkInterface",
"ec2:DetachNetworkInterface",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:ReleaseAddress",
"ec2:UnassignIpv6Addresses",
"ec2:DescribeVpcPeeringConnections",
"logs:CreateLogDelivery",
"logs:GetLogDelivery",
"logs:UpdateLogDelivery",
"logs>DeleteLogDelivery",
"logs:ListLogDeliveries",
"outposts:GetOutpostInstanceTypes"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer stratégies AWS gérées et évoluez ez ez ez ez ez ez ez ez ez ez ez ez ez ez ez ez ez](#)

AWS ElementalMediaConvertFullAccess

AWS ElementalMediaConvertFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AWS Elemental MediaConvert via le SDK AWS Management Console and.

Utilisation de cette stratégie

Vous pouvez AWS ElementalMediaConvertFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 juin 2018, 19:25 UTC
- Heure modifiée : 10 juin 2019, 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaConvertReadOnly

AWSElementalMediaConvertReadOnlyest une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule àAWS Elemental MediaConvert via le SDKAWS Management Console and.

Utilisation de cette stratégie

Vous pouvez les associerAWSElementalMediaConvertReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 juin 2018, 19:25 UTC
- Heure modifiée : 10 juin 2019, 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaLiveFullAccess

AWSElementalMediaLiveFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux MediaLive ressourcesAWS élémentaires

Utilisation de cette stratégie

Vous pouvez AWSElementalMediaLiveFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 8 juillet 2020, 17:07 UTC
- Heure modifiée : 8 juillet 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaLiveReadOnly

AWSElementalMediaLiveReadOnlyest une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux MediaLive ressourcesAWS élémentaires

Utilisation de cette stratégie

Vous pouvezAWSElementalMediaLiveReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 juillet 2020, 16:38 UTC
- Heure modifiée : 8 juillet 2020, 16:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaPackageFullAccess

AWSElementalMediaPackageFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet aux MediaPackage ressources AWS élémentaires

Utilisation de cette stratégie

Vous pouvez les associer AWSElementalMediaPackageFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 décembre 2017, 23:39 UTC
- Heure modifiée : 29 décembre 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaPackageReadOnly

AWSElementalMediaPackageReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux MediaPackage ressources AWS élémentaires

Utilisation de cette stratégie

Vous pouvez les associer AWSElementalMediaPackageReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 décembre 2017, 00:04 UTC
- Heure modifiée : 30 décembre 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS ElementalMediaPackageV2FullAccess

AWS ElementalMediaPackageV2FullAccess est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS ÉlémentaireMediaPackageRessources V2.

Utilisation de cette politique

Vous pouvez joindre AWS ElementalMediaPackageV2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 25 juillet 2023, 20:29 UTC
- Heure de modification : 25 juillet 2023, 20h29 UTC
- ARN: arn:aws:iam::aws:policy/AWS ElementalMediaPackageV2FullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSElementalMediaPackageV2ReadOnly

AWSElementalMediaPackageV2ReadOnlyest un[AWSpolitique gérée](#)qui : Fournit un accès en lecture seule àAWSÉlémentaireMediaPackageRessources V2.

Utilisation de cette politique

Vous pouvez joindreAWSElementalMediaPackageV2ReadOnlyà vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 25 juillet 2023, 20:31 UTC
- Heure de modification :25 juillet 2023, 20h31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSElementalMediaStoreFullAccess

AWSElementalMediaStoreFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet en lecture et en écriture à toutes les MediaStore API

Utilisation de cette stratégie

Vous pouvezAWSElementalMediaStoreFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 5 mars 2018, 23:15 UTC
- Heure modifiée : 5 mars 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaStoreReadOnly

AWSElementalMediaStoreReadOnly est une [politique AWS gérée](#) qui : fournit des autorisations en lecture seule pour les MediaStore API

Utilisation de cette stratégie

Vous pouvez les associer AWSElementalMediaStoreReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 mars 2018, 19:48 UTC
- Heure modifiée : 8 mars 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaTailorFullAccess

AWSElementalMediaTailorFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux MediaTailor ressourcesAWS élémentaires

Utilisation de cette stratégie

Vous pouvezAWSElementalMediaTailorFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 23 novembre 2021, 00:04 UTC
- Heure modifiée : 23 novembre 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSElementalMediaTailorReadOnly

AWSElementalMediaTailorReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux MediaTailor ressources AWS élémentaires

Utilisation de cette stratégie

Vous pouvez les associer AWSElementalMediaTailorReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 novembre 2021, 00:05 UTC
- Heure modifiée : 23 novembre 2021, 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS Enhanced Classic Networking Management Policy

AWS Enhanced Classic Networking Management Policy est une [politique AWS gérée](#) qui : Stratégie visant à activer une fonctionnalité de gestion réseau classique améliorée.

Using this policy

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à des utilisateurs,

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 20 septembre 2017, 17:29 UTC
- Heure modifiée : 20 septembre 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie de Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS](#)

AWSEntityResolutionConsoleFullAccess

AWSEntityResolutionConsoleFullAccess est une [politique AWS gérée](#) qui : fournit à la console un accès complet à AWS Entity Resolution et aux services associés.

Utilisation de cette politique

Vous pouvez vous associer AWSEntityResolutionConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 août 2023, 17:54 UTC
- Heure modifiée : 16 octobre 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "glue:GetSchema",
  "glue:SearchTables",
  "glue:GetSchemaByDefinition",
  "glue:GetSchemaVersion",
  "glue:GetSchemaVersionsDiff",
  "glue:GetDatabase",
  "glue:GetDatabases",
  "glue:GetTable",
  "glue:GetTables",
  "glue:GetTableVersion",
  "glue:GetTableVersions"
],
"Resource" : "*"
},
{
  "Sid" : "S3BucketsConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3SourcesConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:ListBucketVersions",
    "s3:GetBucketVersioning"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TaggingConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues"
  ],
  "Resource" : "*"
},
}
```



```
{
  "Sid" : "KMSConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListRolesToPickRoleForPassing",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PassRoleToEntityResolutionService",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*entityresolution*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "entityresolution.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ManageEventBridgeRules",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:PutTargets",
    "events:PutRule"
  ],
  "Resource" : [
    "arn:aws:events::*:rule/entity-resolution-automatic*"
  ]
},
```

```
{
  "Sid" : "ADXReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "dataexchange:GetDataSet"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess est un [AWS politique gérée](#) qui : fournit un accès en lecture seule à AWS Résolution des entités par le biais du AWS Management Console.

Utilisation de cette politique

Vous pouvez joindre AWSEntityResolutionConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 17 août 2023, 18:18 UTC
- Heure modifiée : 17 août 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorEC2Access

AWSFaultInjectionSimulatorEC2Access est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation dans EC2 et aux autres services requis d'effectuer des actions FIS.

Utilisation de cette politique

Vous pouvez vous associer `AWSFaultInjectionSimulatorEC2Access` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 octobre 2022, 20:39 UTC
- Heure modifiée : 27 novembre 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
```

```

    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : [
      "arn:aws:kms:*:*:key/*"
    ],
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "ec2.*.amazonaws.com"
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      }
    }
  },
  {
    "Sid" : "AllowSSMSendOnEc2",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ssm:*:*:document/*"
    ]
  },
  {
    "Sid" : "AllowSSMStopOnEc2",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:ListCommands"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DescribeInstances",
    "Effect" : "Allow",
    "Action" : "ec2:DescribeInstances",
    "Resource" : "*"
  }
]

```

}

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorECSAccess

AWSFaultInjectionSimulatorECSAccess est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation dans ECS et aux autres services requis d'effectuer des actions FIS.

Utilisation de cette politique

Vous pouvez vous associer AWSFaultInjectionSimulatorECSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 octobre 2022, 20:37 UTC
- Heure modifiée : 25 janvier 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
    }
  ]
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "SSMSend",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
      "arn:aws:ssm:*:*:managed-instance/*",
      "arn:aws:ssm:*:*:document/*"
    ]
  },
  {
    "Sid" : "SSMList",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListCommands",
      "ssm:CancelCommand"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TargetResolutionByTags",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorEKSAccess

AWSFaultInjectionSimulatorEKSAccess est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation dans EKS et aux autres services requis d'effectuer des actions FIS.

Utilisation de cette politique

Vous pouvez vous associer AWSFaultInjectionSimulatorEKSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 octobre 2022, 20:34 UTC
- Heure modifiée : 13 novembre 2023, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorNetworkAccess

AWSFaultInjectionSimulatorNetworkAccess est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation d'effectuer des actions FIS dans le réseau EC2 et aux autres services requis.

Utilisation de cette politique

Vous pouvez vous associer AWSFaultInjectionSimulatorNetworkAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 octobre 2022, 20:32 UTC
- Heure modifiée : 25 janvier 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
```

```
        "ec2:CreateAction" : "CreateNetworkAcl",
        "aws:RequestTag/managedByFIS" : "true"
    }
},
{
    "Sid" : "CreateNetworkAcl",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkAcl",
    "Resource" : "arn:aws:ec2:*:*:network-acl/*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/managedByFIS" : "true"
        }
    }
},
{
    "Sid" : "DeleteNetworkAcl",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/managedByFIS" : "true"
        }
    }
},
{
    "Sid" : "CreateNetworkAclOnVpc",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkAcl",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
    "Sid" : "VpcActions",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVpcs",
```

```

    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeSubnets",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeRouteTables",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGateways"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReplaceNetworkAclAssociation",
  "Effect" : "Allow",
  "Action" : "ec2:ReplaceNetworkAclAssociation",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-acl/*"
  ]
},
{
  "Sid" : "GetManagedPrefixListEntries",
  "Effect" : "Allow",
  "Action" : "ec2:GetManagedPrefixListEntries",
  "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
},
{
  "Sid" : "CreateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:CreateRouteTable",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateRouteTableOnVpc",
  "Effect" : "Allow",
  "Action" : "ec2:CreateRouteTable",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
}

```

```
},
{
  "Sid" : "CreateTagsOnRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateRouteTable",
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateTagsOnNetworkInterface",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface",
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateTagsOnPrefixList",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateManagedPrefixList",
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "DeleteRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
}
```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateRoute",
    "Effect" : "Allow",
    "Action" : "ec2:CreateRoute",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkInterfaceOnSubnet",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group*"
    ]
  },
  {
    "Sid" : "DeleteNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
```

```
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  },
  {
    "Sid" : "CreateManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:CreateManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ModifyManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ReplaceRouteTableAssociation",
    "Effect" : "Allow",
    "Action" : "ec2:ReplaceRouteTableAssociation",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
```



```
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "AssociateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:AssociateRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "DisassociateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:DisassociateRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "DisassociateRouteTableOnSubnet",
  "Effect" : "Allow",
  "Action" : "ec2:DisassociateRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "ModifyVpcEndpointOnRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:ModifyVpcEndpoint",
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "ModifyVpcEndpoint",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ]
  },
  {
    "Sid" : "TransitGatewayRouteTableAssociation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateTransitGatewayRouteTable",
      "ec2:AssociateTransitGatewayRouteTable"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:transit-gateway-route-table/*",
      "arn:aws:ec2:*:*:transit-gateway-attachment/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation dans RDS et aux autres services requis d'effectuer des actions FIS.

Utilisation de cette politique

Vous pouvez vous associer `AWSFaultInjectionSimulatorRDSAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 26 octobre 2022, 20h30 UTC
- Heure modifiée : 13 novembre 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
```

```
    "Effect" : "Allow",
    "Action" : [
      "rds:RebootDBInstance"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:db:*"
    ]
  },
  {
    "Sid" : "DescribeResources",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBClusters",
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TargetResolutionByTags",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess est une [politique AWS gérée](#) qui : Cette politique accorde au service Fault Injection Simulator l'autorisation d'effectuer des actions FIS dans SSM et à d'autres services requis.

Utilisation de cette stratégie

Vous pouvez l'associer `AWSFaultInjectionSimulatorSSMAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 15:33 UTC
- Heure modifiée : 2 juin 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "ssm:StartAutomationExecution"
],
"Resource" : [
  "arn:aws:ssm:*:*:automation-definition/*:*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetAutomationExecution",
    "ssm:StopAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:automation-execution/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListCommands",
    "ssm:CancelCommand"
  ],
  "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarez avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicy est une [politique AWS gérée](#) qui : Politique visant à autoriser l'accès Service AWS aux ressources utilisées ou gérées par Amazon FinSpace

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 12 mai 2023, 16:42 UTC
- Heure modifiée : 1 décembre 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
```

```
        "AWS/Usage"
      ]
    }
  },
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSFMAdminFullAccess

AWSFMAdminFullAccess est une [politique AWS gérée](#) qui : Accès complet pour AWS FM Administrator

Utilisation de cette stratégie

Vous pouvez AWSFMAdminFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 mai 2018, 18:06 UTC
- Heure modifiée : 20 octobre 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
```

```
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fms.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "fms.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess est une [politique AWS gérée](#) qui : Accès en lecture seule pour AWS FM Administrator qui permet de surveiller les opérations AWS FM

Utilisation de cette stratégie

Vous pouvez AWSFMAdminReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 mai 2018, 20:07 UTC
- Heure modifiée : 31 octobre 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",

```

```

    "organizations:DescribeAccount",
    "organizations:ListRoots",
    "organizations:ListChildren",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListOrganizationalUnitsForParent",
    "shield:GetSubscriptionState",
    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListAvailableManagedRuleGroups",
    "wafv2:CheckCapacity",
    "wafv2:ListAvailableManagedRuleGroupVersions",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:DescribeRuleGroupMetadata",
    "network-firewall:ListRuleGroups",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "fms.amazonaws.com"
      ]
    }
  }
}
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess` est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule aux actionsAWS WAF pour les comptes membres deAWS Firewall Manager

Utilisation de cette stratégie

Vous pouvez les associer `AWSFMMemberReadOnlyAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 mai 2018, 21:05 UTC
- Heure modifiée : 9 mai 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSForWordPressPluginPolicy

AWSForWordPressPluginPolicy est une [politique AWS gérée](#) qui : Politique gérée pour le plugin AWS For Wordpress

Utilisation de cette stratégie

Vous pouvez AWSForWordPressPluginPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 30 octobre 2019, 00:27 UTC
- Heure modifiée : 20 janvier 2020, 23 h 20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*"
      ]
    }
  ]
}
```

```
    "arn:aws:s3:::audio-for-wordpress*"
  ]
},
{
  "Sid" : "Permissions3",
  "Effect" : "Allow",
  "Action" : [
    "acm:AddTagsToCertificate",
    "acm:DescribeCertificate",
    "acm:RequestCertificate",
    "cloudformation:CreateStack",
    "cloudfront:ListDistributions"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{
  "Sid" : "Permissions4",
  "Effect" : "Allow",
  "Action" : [
    "acm>DeleteCertificate",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:UpdateStack",
    "cloudfront:CreateDistribution",
    "cloudfront:CreateInvalidation",
    "cloudfront>DeleteDistribution",
    "cloudfront:GetDistribution",
    "cloudfront:GetInvalidation",
    "cloudfront:TagResource",
    "cloudfront:UpdateDistribution"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
    }
  }
}
```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGitSyncServiceRolePolicy

AWSGitSyncServiceRolePolicy est une [politique AWS gérée](#) qui : Politique qui permet à AWS Code Connections de synchroniser le contenu de votre dépôt git

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 16 novembre 2023, 17:05 UTC
- Heure modifiée : 16 novembre 2023, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSGlobalAcceleratorSLRPolicy

AWSGlobalAcceleratorSLRPolicy est une [politique AWS gérée qui : Politique](#) accordant des autorisations à AWS Global Accelerator pour gérer les interfaces réseau élastiques et les groupes de sécurité EC2.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service

- Heure de création : 05 avril 2019, 19:39 UTC
- Heure modifiée : 12 septembre 2023, 16h45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
      }
    }
  },
  {
    "Sid" : "EC2Action3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ElbAction1",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeListeners",
      "elasticloadbalancing:DescribeTargetGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2Action4",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:network-interface/*"
    ]
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSGlueConsoleFullAccess

AWSGlueConsoleFullAccess est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS Collez via le AWS Management Console

Utilisation de cette politique

Vous pouvez joindre AWSGlueConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 14 août 2017, 13:37 UTC
- Heure de modification : 14 juillet 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",

```

```

    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeDBSubnetGroups",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "cloudformation:ListStacks",
    "cloudformation:DescribeStacks",
    "cloudformation:GetTemplateSummary",
    "dynamodb:ListTables",
    "kms:ListAliases",
    "kms:DescribeKey",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListDashboards",
    "databrew:ListRecipes",
    "databrew:ListRecipeVersions",
    "databrew:DescribeRecipe"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/*aws-glue-*/**",

```

```
    "arn:aws:s3:::aws-glue-*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
```

```

    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
    },
    "StringEquals" : {
      "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam:*:*:role/AWSGlueServiceRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
},
{

```



```
"Action" : [
  "iam:PassRole"
],
"Effect" : "Allow",
"Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : [
      "ec2.amazonaws.com"
    ]
  }
}
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSGlueConsoleSageMakerNotebookFullAccess

AWSGlueConsoleSageMakerNotebookFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AWS Glue via les instances de bloc-notes de Sagemaker AWS Management Console et un accès à celles-ci.

Utilisation de cette stratégie

Vous pouvez AWSGlueConsoleSageMakerNotebookFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 5 octobre 2018, 17:52 UTC
- Heure modifiée : 15 juillet 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
```

```
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:CreateNetworkInterface",
    "ec2:AttachNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNetworkInterfaces",
    "rds:DescribeDBInstances",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "cloudformation:DescribeStacks",
    "cloudformation:GetTemplateSummary",
    "dynamodb:ListTables",
    "kms:ListAliases",
    "kms:DescribeKey",
    "sagemaker:ListNotebookInstances",
    "cloudformation:ListStacks",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListDashboards"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ]
},
```

```

    "Resource" : [
      "arn:aws:s3::*/*aws-glue-*/*",
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:/aws-glue/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreatePresignedNotebookInstanceUrl",
      "sagemaker:CreateNotebookInstance",
      "sagemaker>DeleteNotebookInstance",
      "sagemaker:DescribeNotebookInstance",
      "sagemaker:StartNotebookInstance",
      "sagemaker:StopNotebookInstance",
      "sagemaker:UpdateNotebookInstance",
      "sagemaker:ListTags"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
  }

```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker>CreateNotebookInstanceLifecycleConfig",
        "sagemaker>DeleteNotebookInstanceLifecycleConfig",
        "sagemaker>ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2>DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    }
  ]
}

```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : [
        "aws-glue-*"
      ]
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
}

```

```
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AwsGlueDataBrewFullAccessPolicy

AwsGlueDataBrewFullAccessPolicy est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS Glue DataBrew via la AWS Management Console. Fournit également un accès sélectif à des services connexes (par exemple, S3, KMS, Glue).

Utilisation de cette stratégie

Vous pouvez associer AwsGlueDataBrewFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 novembre 2020, 16:51 UTC
- Heure modifiée : 4 février 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew>DeleteDataset",
```



```
"databrew:CreateProject",
"databrew:DescribeProject",
"databrew:ListProjects",
"databrew:StartProjectSession",
"databrew:SendProjectSessionAction",
"databrew:UpdateProject",
"databrew>DeleteProject",
"databrew:CreateRecipe",
"databrew:DescribeRecipe",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:PublishRecipe",
"databrew:UpdateRecipe",
"databrew:BatchDeleteRecipeVersion",
"databrew>DeleteRecipeVersion",
"databrew:CreateRecipeJob",
"databrew:CreateProfileJob",
"databrew:DescribeJob",
"databrew:DescribeJobRun",
"databrew:ListJobRuns",
"databrew:ListJobs",
"databrew:StartJobRun",
"databrew:StopJobRun",
"databrew:UpdateProfileJob",
"databrew:UpdateRecipeJob",
"databrew>DeleteJob",
"databrew:CreateSchedule",
"databrew:DescribeSchedule",
"databrew:ListSchedules",
"databrew:UpdateSchedule",
"databrew>DeleteSchedule",
"databrew:CreateRuleset",
"databrew>DeleteRuleset",
"databrew:DescribeRuleset",
"databrew:ListRulesets",
"databrew:UpdateRuleset",
"databrew:ListTagsForResource",
"databrew:TagResource",
"databrew:UntagResource"
],
"Resource" : [
  "*"
]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "appflow:DescribeFlow",
    "appflow:DescribeFlowExecutionRecords",
    "appflow:ListFlows",
    "glue:GetConnection",
    "glue:GetConnections",
    "glue:GetDatabases",
    "glue:GetPartitions",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetDataCatalogEncryptionSettings",
    "dataexchange:ListDataSets",
    "dataexchange:ListDataSetRevisions",
    "dataexchange:ListRevisionAssets",
    "dataexchange:CreateJob",
    "dataexchange:StartJob",
    "dataexchange:GetJob",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSubnetGroups",
    "redshift-data:DescribeStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "sts:GetCallerIdentity",
    "cloudtrail:LookupEvents",
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateConnection"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:GetDatabases"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
    ]
},
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateDataKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateRandom"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "databrew.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
```

```
"Action" : [
  "secretsmanager:CreateSecret"
],
"Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
"Condition" : {
  "StringLike" : {
    "secretsmanager:Name" : "databrew!default"
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "databrew.amazonaws.com"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "databrew.amazonaws.com"
      ]
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGlueDataBrewServiceRole

AWSGlueDataBrewServiceRole est une [politique AWS gérée](#) qui : cette politique autorise Glue à effectuer des actions sur le catalogue de données Glue de l'utilisateur, elle autorise également les actions ec2 pour permettre à Glue de créer ENI pour se connecter aux ressources du VPC, autorise également Glue à accéder aux données enregistrées dans Lakeformation et autorise à accéder à Cloudwatch de l'utilisateur

Utilisation de cette politique

Vous pouvez vous associer AWSGlueDataBrewServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 04 décembre 2020, 21:26 UTC
- Heure modifiée : 20 mars 2024, 23h28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
```

```
    "glue:GetTables",
    "glue:GetConnection"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "GluePIIPermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:BatchGetCustomEntityTypes",
    "glue:GetCustomEntityType"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "S3PublicDatasetAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::databrew-public-datasets-*"
  ]
},
{
  "Sid" : "EC2NetworkingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
  },
  {
    "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws-glue-service-resource" : "*"
      }
    },
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "EC2GlueTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "aws-glue-service-resource"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group*"
    ]
  },
  {
    "Sid" : "GlueDatabrewLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
    ]
  }
]
```



```
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSGlueSchemaRegistryFullAccess

AWSGlueSchemaRegistryFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet au service AWS Glue Schema Registry

Utilisation de cette stratégie

Vous pouvez AWSGlueSchemaRegistryFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : politique AWS gérée

- Heure de création : 20 novembre 2020, 00:19 UTC
- Heure modifiée : 20 novembre 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue>DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue>DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue>DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetTags",
      "glue:TagResource",
      "glue:UntagResource"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:schema/*",
      "arn:aws:glue:*:*:registry/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGlueSchemaRegistryReadOnlyAccess

AWSGlueSchemaRegistryReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule au service de registreAWS Glue Schema

Utilisation de cette stratégie

Vous pouvezAWSGlueSchemaRegistryReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politiqueAWS gérée
- Heure de création : 20 novembre 2020, 00:20 UTC
- Heure modifiée : 20 novembre 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGlueServiceNotebookRole

AWSGlueServiceNotebookRoleest une [politique AWS gérée](#) qui : le rôle de service Policy for AWS Glue qui permet au client de gérer le serveur de blocs-notes

Utilisation de cette politique

Vous pouvez vous associer AWSGlueServiceNotebookRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 14 août 2017, 13:37 UTC
- Heure modifiée : 9 octobre 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateDatabase",
      "glue:CreatePartition",
      "glue:CreateTable",
      "glue>DeleteDatabase",
      "glue>DeletePartition",
      "glue>DeleteTable",
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetTable",
      "glue:GetTableVersions",
      "glue:GetTables",
      "glue:UpdateDatabase",
      "glue:UpdatePartition",
      "glue:UpdateTable",
      "glue:CreateConnection",
      "glue:CreateJob",
      "glue>DeleteConnection",
      "glue>DeleteJob",
      "glue:GetConnection",
      "glue:GetConnections",
      "glue:GetDevEndpoint",
      "glue:GetDevEndpoints",
      "glue:GetJob",
      "glue:GetJobs",
      "glue:UpdateJob",
      "glue:BatchDeleteConnection",
      "glue:UpdateConnection",
      "glue:GetUserDefinedFunction",
      "glue:UpdateUserDefinedFunction",
      "glue:GetUserDefinedFunctions",
      "glue>DeleteUserDefinedFunction",
      "glue:CreateUserDefinedFunction",
      "glue:BatchGetPartition",
      "glue:BatchDeletePartition",
      "glue:BatchCreatePartition",
      "glue:BatchDeleteTable",
      "glue:UpdateDevEndpoint",
```

```
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "codewhisperer:GenerateRecommendations"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*",
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  }
},
  "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSGlueServiceRole

AWSGlueServiceRole est une [politique AWS gérée](#) qui : le rôle de service Policy for AWS Glue qui permet d'accéder aux services connexes, notamment EC2, S3 et Cloudwatch Logs

Utilisation de cette politique

Vous pouvez vous associer AWSGlueServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 14 août 2017, 13:37 UTC
- Heure modifiée : 11 septembre 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/*",
    "arn:aws:s3:::*/*aws-glue-*/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*",
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:*:/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  }
}
```

```
    }
  },
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy est une [politique AWS gérée](#) qui : fournit des autorisations permettant aux utilisateurs de créer et d'utiliser uniquement les sessions de bloc-notes associées à l'utilisateur. Cette politique inclut également des autorisations permettant explicitement aux utilisateurs de transmettre un rôle de session Glue restreint.

Utilisation de cette politique

Vous pouvez vous associer AwsGlueSessionUserRestrictedNotebookPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 avril 2022, 15:24 UTC
- Heure modifiée : 22 novembre 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    }
  ]
}
```

```
},
{
  "Sid" : "NotebookAllowActions2",
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
    }
  }
},
{
  "Sid" : "NotebookAllowActions3",
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "NotebookDenyActions",
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ]
},
```

```

    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    },
  ],
  {
    "Sid" : "NotebookPassRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
      AwsGlueSessionServiceRoleUserRestrictedForNotebook*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

AwsGlueSessionUserRestrictedNotebookServiceRole est une [stratégie AWS gérée](#) qui : fournit un un un un un un un un accès à toutes les ressources AWS Glue sauf pour les séances.

Permet aux utilisateurs de créer et d'utiliser uniquement les séances de bloc-notes associées à l'utilisateur. Cette politique inclut également d'autres autorisations requises par AWS Glue pour gérer les ressources Glue dans d'autres AWS services.

Utilisation de cette politique.

Vous pouvez `AwsGlueSessionUserRestrictedNotebookServiceRole` les associer à vos utilisateurs, groupes et rôles.

Détails des détails de détails

- Type : Politique de rôle de service
- Heure de création : 18 avril 2022, 15:27 UTC
- Heure modifiée : 18 avril 2022, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la version qui définit les autorisations pour la de la de de la version par pour la version par la version qui définit les autorisations pour la la Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",

```

```

    "arn:aws:glue:*:*:connection/*",
    "arn:aws:glue:*:*:userDefinedFunction/*",
    "arn:aws:glue:*:*:devEndpoint/*",
    "arn:aws:glue:*:*:job/*",
    "arn:aws:glue:*:*:trigger/*",
    "arn:aws:glue:*:*:crawler/*",
    "arn:aws:glue:*:*:workflow/*",
    "arn:aws:glue:*:*:mlTransform/*",
    "arn:aws:glue:*:*:registry/*",
    "arn:aws:glue:*:*:schema/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ]
}

```



```
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:ListSessions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "glue:TagResource",
      "glue:UntagResource",
      "tag:TagResources",
      "tag:UntagResources"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  },
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/**aws-glue-*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  }
}
```

```
    },
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'une autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer vers les autorisations de moindre privilège et AWS évoluer vers les autorisations de moindre privilège et évoluer vers les autorisations de moindre privilège](#)

AwsGlueSessionUserRestrictedPolicy

AwsGlueSessionUserRestrictedPolicy est une [stratégie AWS gérée](#) qui : fournit des autorisations qui permettent aux utilisateurs de créer et d'utiliser uniquement les séances interactives associées à l'utilisateur. Cette politique inclut également des autorisations permettant explicitement aux utilisateurs de passer un rôle de séance GlueSessionGlueSessionGlue restreint.

Utilisation de cette politique

Vous pouvez AwsGlueSessionUserRestrictedPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 14 avril 2022, 21:31 UTC
- Heure modifiée : 14 avril 2022, 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est celle qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue>DeleteSession",
        "glue:GetSession"
      ],
    }
  ],
}
```

```
"Resource" : [
  "arn:aws:glue:*:*:session/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/owner" : "${aws:userid}"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
  ]
}
```

```
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AwsGlueSessionUserRestrictedServiceRole

AwsGlueSessionUserRestrictedServiceRole est une [stratégieAWS gérée](#) qui : fournit un accès complet à toutes ressourcesAWS Glue sauf pour les séances. Permet aux utilisateurs de créer et d'utiliser uniquement les séances interactives associées à l'utilisateur. Cette politique inclut également d'autres autorisations requises parAWS Glue autres services Glue d'autresAWS services.

Utilisation de cette politique de politique de

Vous pouvezAwsGlueSessionUserRestrictedServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails de la politique de

- Type : Politique de rôle de service
- Heure de création : 14 avril 2022, 21:30 UTC
- Heure modifiée : 14 avril 2022, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie de stratégie de stratégie

```
{
  "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" : "${aws:userid}"
  },
  "ForAnyValue:StringEquals" : {
    "aws:TagKeys" : [
      "owner"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/owner" : "${aws:userid}"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
```



```
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/*aws-glue-*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*"
  ]
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents"
],
"Resource" : [
  "arn:aws:logs:*:*:/aws-glue/*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  },
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM IAM IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège](#)

AWSGrafanaAccountAdministrator

AWSGrafanaAccountAdministrator est une [politique AWS gérée](#) qui : fournit un accès au sein d'Amazon Grafana pour créer et gérer des espaces de travail pour l'ensemble de l'organisation.

Utilisation de cette stratégie

Vous pouvez AWSGrafanaAccountAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 février 2021, 00:20 UTC
- Heure modifiée : 15 février 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Sid" : "GrafanaIAMGetRolePermission",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "AWSGrafanaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "grafana:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GrafanaIAMPassRolePermission",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "grafana.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGrafanaConsoleReadOnlyAccess

AWSGrafanaConsoleReadOnlyAccess est une [politique AWS gérée](#) qui : Accès aux opérations en lecture seule dans Amazon Grafana.

Utilisation de cette stratégie

Vous pouvez les associer `AWSGrafanaConsoleReadOnlyAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 février 2021, 00:10 UTC
- Heure modifiée : 15 février 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGrafanaWorkspacePermissionManagement

AWSGrafanaWorkspacePermissionManagementest une [politiqueAWS gérée](#) qui : permet uniquement de mettre à jour les autorisations des utilisateurs et des groupes pour les espaces de travailAWS Grafana.

Utilisation de cette stratégie

Vous pouvezAWSGrafanaWorkspacePermissionManagement les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 23 février 2021, 00:15 UTC
- Heure modifiée : 15 mars 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AWSGrafanaPermissions",
    "Effect" : "Allow",
    "Action" : [
      "grafana:DescribeWorkspace",
      "grafana:DescribeWorkspaceAuthentication",
      "grafana:UpdatePermissions",
      "grafana:ListPermissions",
      "grafana:ListWorkspaces"
    ],
    "Resource" : "arn:aws:grafana:*:*:/workspaces*"
  },
  {
    "Sid" : "IAMIdentityCenterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sso:DescribeRegisteredRegions",
      "sso:GetSharedSsoConfiguration",
      "sso:ListDirectoryAssociations",
      "sso:GetManagedApplicationInstance",
      "sso:ListProfiles",
      "sso:AssociateProfile",
      "sso:DisassociateProfile",
      "sso:GetProfile",
      "sso:ListProfileAssociations",
      "sso-directory:DescribeUser",
      "sso-directory:DescribeGroup"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGrafanaWorkspacePermissionManagementV2

AWSGrafanaWorkspacePermissionManagementV2 est une [politique AWS gérée](#) qui : permet de mettre à jour les autorisations des utilisateurs et des groupes IAM Identity Center (iDC) pour les espaces de travail Grafana gérés par Amazon.

Utilisation de cette politique

Vous pouvez vous associer AWSGrafanaWorkspacePermissionManagementV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 janvier 2024, 18:39 UTC
- Heure modifiée : 5 janvier 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
```



```
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
    ],
    "Resource" : "arn:aws:grafana:*:*:/workspaces*"
},
{
    "Sid" : "IAMIdentityCenterPermissions",
    "Effect" : "Allow",
    "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSGreengrassFullAccess

AWSGreengrassFullAccess est une [politique AWS gérée](#) qui : Cette politique donne un accès complet aux actions de configuration, de gestion et de déploiement de AWS Greengrass

Utilisation de cette stratégie

Vous pouvez `AWSGreengrassFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 mai 2017, 00:47 UTC
- Heure modifiée : 3 mai 2017, 00:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGreengrassReadOnlyAccess

AWSGreengrassReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique donne un accès en lecture seule aux actions de configuration, de gestion et de déploiement de AWS Greengrass

Utilisation de cette stratégie

Vous pouvez les associer AWSGreengrassReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 octobre 2018, 16:01 UTC
- Heure modifiée : 30 octobre 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGreengrassResourceAccessRolePolicy

AWSGreengrassResourceAccessRolePolicyest une [politiqueAWS gérée qui : Politique](#) pour le rôle de serviceAWS Greengrass qui permet d'accéder à des services connexes, y comprisAWS Lambda etAWS IoT Thing Shadows.

Utilisation de cette stratégie

Vous pouvezAWSGreengrassResourceAccessRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 février 2017, 21:17 UTC
- Heure modifiée : 14 novembre 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "AllowGreengrassToGetLambdaFunctions",
    "Action" : [
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowGreengrassToGetGreengrassSecrets",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
  },
  {
    "Sid" : "AllowGreengrassAccessToS3Objects",
    "Action" : [
      "s3:GetObject"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:s3::*Greengrass*",
      "arn:aws:s3::*GreenGrass*",
      "arn:aws:s3::*greengrass*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Sid" : "AllowGreengrassAccessToS3BucketLocation",
    "Action" : [
      "s3:GetBucketLocation"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
    "Action" : [
```

```
    "sagemaker:DescribeTrainingJob"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy est une [politique AWS gérée](#) qui : fournit à l'instance de point de terminaison Dataflow les autorisations nécessaires pour utiliser l'agent AWS Ground Station

Utilisation de cette stratégie

Vous pouvez les associer AWSGroundStationAgentInstancePolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 mars 2023, 15:23 UTC
- Heure modifiée : 29 mars 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSHealth_EventProcessorServiceRolePolicy

AWSHealth_EventProcessorServiceRolePolicy est une [politique AWS gérée](#) qui :
Autorise AWS Health à activer la fonction de processeur d'événements Health.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 janvier 2023, 19:24 UTC
- Heure modifiée : 13 janvier 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSHealthFullAccess

AWSHealthFullAccess est une [politiqueAWS gérée](#) qui : accorde un accès complet auxAWS API et notifications, ainsi qu'à Personal Health Dashboard.

Utilisation de cette politique

Vous pouvezAWSHealthFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 décembre 2016, 12h30 UTC
- Heure modifiée : 16 novembre 2020, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSHealthImagingFullAccess

AWSHealthImagingFullAccess est un [AWS politique gérée](#) qui : Fournit un accès complet à AWS Service d'imagerie médicale.

Utilisation de cette politique

Vous pouvez joindre AWSHealthImagingFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 25 juillet 2023, 23:39 UTC
- Heure modifiée : 25 juillet 2023, 23h39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "medical-imaging:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "medical-imaging.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess est un [AWS politique gérée](#) qui : Fournit un accès en lecture seule à AWS Service d'imagerie médicale.

Utilisation de cette politique

Vous pouvez joindre AWSHealthImagingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 25 juillet 2023, 23 h 40 UTC
- Heure de modification :1 août 2023, 15h18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

Version de la politique

Version de la politique : v2(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec des politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSIAMIdentityCenterAllowListForIdentityContext

`AWSIAMIdentityCenterAllowListForIdentityContext` est une [politique AWS gérée](#) qui : fournit la liste des actions autorisées pour les rôles assumés dans le contexte d'identité IAM Identity Center. AWS Le Security Token Service (AWSSTS) associe automatiquement cette politique aux rôles assumés. Le contexte d'identité est transmis en tant que `ProvidedContext`.

Utilisation de cette politique

Vous pouvez vous associer `AWSIAMIdentityCenterAllowListForIdentityContext` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 novembre 2023, 15:21 UTC
- Heure modifiée : 25 novembre 2023, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena>DeleteNamedQuery",
        "athena>DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
```



```
"glue:GetPartition",
"glue:GetPartitions",
"glue:BatchGetPartition",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:SearchTables",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue>DeleteDatabase",
"glue:CreateTable",
"glue>DeleteTable",
"glue:BatchDeleteTable",
"glue:UpdateTable",
"glue:BatchCreatePartition",
"glue:CreatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:UpdatePartition",
"glue:BatchUpdatePartition",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"lakeformation:GetDataAccess",
"s3:GetAccessGrantsInstanceForPrefix",
"s3:GetDataAccess"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess est une [politique AWS gérée](#) qui : Accorde un accès complet au service Identity Sync

Utilisation de cette stratégie

Vous pouvez AWSIdentitySyncFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 mars 2022, 23:29 UTC
- Heure modifiée : 23 mars 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "identity-sync:DeleteSyncProfile",
    "identity-sync:CreateSyncProfile",
    "identity-sync:GetSyncProfile",
    "identity-sync:StartSync",
    "identity-sync:StopSync",
    "identity-sync:CreateSyncFilter",
    "identity-sync>DeleteSyncFilter",
    "identity-sync:ListSyncFilters",
    "identity-sync:CreateSyncTarget",
    "identity-sync>DeleteSyncTarget",
    "identity-sync:GetSyncTarget",
    "identity-sync:UpdateSyncTarget"
  ],
  "Resource" : "arn:*:identity-sync:*:*:*/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIdentitySyncReadOnlyAccess

AWSIdentitySyncReadOnlyAccess est une [politique AWS gérée](#) qui : Accès en lecture seule au service Identity Sync

Utilisation de cette stratégie

Vous pouvez AWSIdentitySyncReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 mars 2022, 23:29 UTC
- Heure modifiée : 23 mars 2022, 23:29 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSImageBuilderFullAccess

`AWSImageBuilderFullAccess` est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les actions AWS d'Image Builder et un accès limité aux ressources aux AWS services associés.

Utilisation de cette stratégie

Vous pouvez les associer `AWSImageBuilderFullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des stratégies

- Type : politique AWS gérée
- Heure de création : 20 décembre 2019, 18:25 UTC
- Heure modifiée : 13 avril 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:ListLicenseConfigurations",
      "license-manager:ListLicenseSpecificationsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetInstanceProfile"
    ],
    "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:instance-profile/*imagebuilder*",
      "arn:aws:iam::*:role/*imagebuilder*"
    ]
  },

```

```

    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : "arn:aws:s3:::*:imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVpcs",
      "ec2:DescribeRegions",
      "ec2:DescribeVolumes",
      "ec2:DescribeSubnets",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeInstanceTypeOfferings",

```

```
    "ec2:DescribeLaunchTemplates"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSImageBuilderReadOnlyAccess

AWSImageBuilderReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule à toutes les actionsAWS d'Image Builder.

Utilisation de cette stratégie

Vous pouvezAWSImageBuilderReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 19 décembre 2019, 22:29 UTC
- Heure modifiée : 19 décembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSImportExportFullAccess

`AWSImportExportFullAccess` est une [politique AWS gérée](#) qui : fournit un accès en lecture et en écriture aux tâches créées dans le cadre du Compte AWS.

Utilisation de cette stratégie

Vous pouvez `AWSImportExportFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSImportExportReadOnlyAccess

`AWSImportExportReadOnlyAccess` est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux tâches créées dans le cadre du Compte AWS.

Utilisation de cette stratégie

Vous pouvez `AWSImportExportReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

AWSIncidentManagerIncidentAccessServiceRolePolicy est une [politique AWS gérée](#) qui : accorde au gestionnaire d'incidents l'autorisation d'appeler d'autres AWS services dans le cadre de la gestion d'un incident.

Utilisation de cette politique

Vous pouvez vous associer AWSIncidentManagerIncidentAccessServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2023, 00:01 UTC
- Heure modifiée : 20 février 2024, 23h02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSIncidentManagerResolverAccess

AWSIncidentManagerResolverAccess est une [politique AWS gérée](#) qui : Cette politique accorde l'autorisation de démarrer, de visualiser et de mettre à jour des incidents avec un accès complet à la chronologie personnalisée des événements et aux éléments connexes. Attribuez cette politique aux utilisateurs qui créeront et résoudront les incidents.

Utilisation de cette stratégie

Vous pouvez les associer AWSIncidentManagerResolverAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 10 mai 2021, 06:12 UTC
- Heure modifiée : 10 mai 2021, 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "ssm-incidents:ListIncidentRecords",
  "ssm-incidents:GetIncidentRecord",
  "ssm-incidents:UpdateIncidentRecord",
  "ssm-incidents:ListTimelineEvents",
  "ssm-incidents:CreateTimelineEvent",
  "ssm-incidents:GetTimelineEvent",
  "ssm-incidents:UpdateTimelineEvent",
  "ssm-incidents>DeleteTimelineEvent",
  "ssm-incidents:ListRelatedItems",
  "ssm-incidents:UpdateRelatedItems"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIncidentManagerServiceRolePolicy

AWSIncidentManagerServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique autorise Incident Manager à gérer les enregistrements des incidents et les ressources associées en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 10 mai 2021, 03:34 UTC

- Heure modifiée : 5 décembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    }
  ],
}
```



```
{
  "Sid" : "PutMetricDataPermission",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/IncidentManager"
    }
  }
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer AWS avec politiques de moindre privilège](#)

AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS IoT 1-Click.

Utilisation de cette stratégie

Vous pouvez AWSIoT1ClickFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 mai 2018, 22:10 UTC
- Heure modifiée : 11 mai 2018, 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule àAWS IoT 1-Click.

Utilisation de cette stratégie

Vous pouvezAWSIoT1ClickReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 mai 2018, 21:49 UTC
- Heure modifiée : 11 mai 2018, 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTAnalyticsFullAccess

AWSIoTAnalyticsFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à IoT Analytics.

Utilisation de cette stratégie

Vous pouvez les associer AWSIoTAnalyticsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 18 juin 2018, 23:02 UTC
- Heure modifiée : 18 juin 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTAnalyticsReadOnlyAccess

AWSIoTAnalyticsReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à IoT Analytics.

Utilisation de cette stratégie

Vous pouvezAWSIoTAnalyticsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 18 juin 2018, 21:37 UTC
- Heure modifiée : 18 juin 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "iotanalytics:Describe*",
      "iotanalytics:List*",
      "iotanalytics:Get*",
      "iotanalytics:SampleChannelData"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTConfigAccess

AWSIoTConfigAccess est une [politiqueAWS gérée](#) qui : Cette politique donne un accès complet aux actions de configuration de l'AWSIoT

Utilisation de cette stratégie

Vous pouvezAWSIoTConfigAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 octobre 2015, 21:52 UTC
- Heure modifiée : 27 septembre 2019, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

Version de la politique

Version de la politique :v9 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot>DeleteAuthorizer",
        "iot>DeleteCACertificate",
        "iot>DeleteCertificate",
        "iot>DeleteJob",
        "iot>DeleteJobExecution",
        "iot>DeleteOTAUpdate",
        "iot>DeletePolicy",
        "iot>DeletePolicyVersion",
```

```
"iot:DeleteRegistrationCode",
"iot:DeleteRoleAlias",
"iot:DeleteStream",
"iot:DeleteThing",
"iot:DeleteThingGroup",
"iot:DeleteThingType",
"iot:DeleteTopicRule",
"iot:DeleteV2LoggingLevel",
"iot:DeprecateThingType",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeDefaultAuthorizer",
"iot:DescribeEndpoint",
"iot:DescribeEventConfigurations",
"iot:DescribeIndex",
"iot:DescribeJob",
"iot:DescribeJobExecution",
"iot:DescribeRoleAlias",
"iot:DescribeStream",
"iot:DescribeThing",
"iot:DescribeThingGroup",
"iot:DescribeThingRegistrationTask",
"iot:DescribeThingType",
"iot:DetachPolicy",
"iot:DetachPrincipalPolicy",
"iot:DetachThingPrincipal",
"iot:DisableTopicRule",
"iot:EnableTopicRule",
"iot:GetEffectivePolicies",
"iot:GetIndexingConfiguration",
"iot:GetJobDocument",
"iot:GetLoggingOptions",
"iot:GetOTAUpdate",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:GetRegistrationCode",
"iot:GetTopicRule",
"iot:GetV2LoggingOptions",
"iot:ListAttachedPolicies",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCertificatesByCA",
```



```
"iot:ListIndices",
"iot:ListJobExecutionsForJob",
"iot:ListJobExecutionsForThing",
"iot:ListJobs",
"iot:ListOTAUpdates",
"iot:ListOutgoingCertificates",
"iot:ListPolicies",
"iot:ListPolicyPrincipals",
"iot:ListPolicyVersions",
"iot:ListPrincipalPolicies",
"iot:ListPrincipalThings",
"iot:ListRoleAliases",
"iot:ListStreams",
"iot:ListTargetsForPolicy",
"iot:ListThingGroups",
"iot:ListThingGroupsForThing",
"iot:ListThingPrincipals",
"iot:ListThingRegistrationTaskReports",
"iot:ListThingRegistrationTasks",
"iot:ListThings",
"iot:ListThingsInThingGroup",
"iot:ListThingTypes",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:RegisterCACertificate",
"iot:RegisterCertificate",
"iot:RegisterThing",
"iot:RejectCertificateTransfer",
"iot:RemoveThingFromThingGroup",
"iot:ReplaceTopicRule",
"iot:SearchIndex",
"iot:SetDefaultAuthorizer",
"iot:SetDefaultPolicyVersion",
"iot:SetLoggingOptions",
"iot:SetV2LoggingLevel",
"iot:SetV2LoggingOptions",
"iot:StartThingRegistrationTask",
"iot:StopThingRegistrationTask",
"iot:TestAuthorization",
"iot:TestInvokeAuthorizer",
"iot:TransferCertificate",
"iot:UpdateAuthorizer",
"iot:UpdateCACertificate",
"iot:UpdateCertificate",
```

```

    "iot:UpdateEventConfigurations",
    "iot:UpdateIndexingConfiguration",
    "iot:UpdateRoleAlias",
    "iot:UpdateStream",
    "iot:UpdateThing",
    "iot:UpdateThingGroup",
    "iot:UpdateThingGroupsForThing",
    "iot:UpdateAccountAuditConfiguration",
    "iot:DescribeAccountAuditConfiguration",
    "iot>DeleteAccountAuditConfiguration",
    "iot:StartOnDemandAuditTask",
    "iot:CancelAuditTask",
    "iot:DescribeAuditTask",
    "iot:ListAuditTasks",
    "iot:CreateScheduledAudit",
    "iot:UpdateScheduledAudit",
    "iot>DeleteScheduledAudit",
    "iot:DescribeScheduledAudit",
    "iot:ListScheduledAudits",
    "iot:ListAuditFindings",
    "iot:CreateSecurityProfile",
    "iot:DescribeSecurityProfile",
    "iot:UpdateSecurityProfile",
    "iot>DeleteSecurityProfile",
    "iot:AttachSecurityProfile",
    "iot:DetachSecurityProfile",
    "iot:ListSecurityProfiles",
    "iot:ListSecurityProfilesForTarget",
    "iot:ListTargetsForSecurityProfile",
    "iot:ListActiveViolations",
    "iot:ListViolationEvents",
    "iot:ValidateSecurityProfileBehaviors"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTConfigReadOnlyAccess

AWSIoTConfigReadOnlyAccess est une [politiqueAWS gérée](#) qui : Cette politique donne un accès en lecture seule aux actions de configuration de l'IoT

Utilisation de cette stratégie

Vous pouvez AWSIoTConfigReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 octobre 2015, 21:52 UTC
- Heure modifiée : 27 septembre 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
```

```
"iot:DescribeEndpoint",
"iot:DescribeEventConfigurations",
"iot:DescribeIndex",
"iot:DescribeJob",
"iot:DescribeJobExecution",
"iot:DescribeRoleAlias",
"iot:DescribeStream",
"iot:DescribeThing",
"iot:DescribeThingGroup",
"iot:DescribeThingRegistrationTask",
"iot:DescribeThingType",
"iot:GetEffectivePolicies",
"iot:GetIndexingConfiguration",
"iot:GetJobDocument",
"iot:GetLoggingOptions",
"iot:GetOTAUpdate",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:GetRegistrationCode",
"iot:GetTopicRule",
"iot:GetV2LoggingOptions",
"iot:ListAttachedPolicies",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCertificatesByCA",
"iot:ListIndices",
"iot:ListJobExecutionsForJob",
"iot:ListJobExecutionsForThing",
"iot:ListJobs",
"iot:ListOTAUpdates",
"iot:ListOutgoingCertificates",
"iot:ListPolicies",
"iot:ListPolicyPrincipals",
"iot:ListPolicyVersions",
"iot:ListPrincipalPolicies",
"iot:ListPrincipalThings",
"iot:ListRoleAliases",
"iot:ListStreams",
"iot:ListTargetsForPolicy",
"iot:ListThingGroups",
"iot:ListThingGroupsForThing",
"iot:ListThingPrincipals",
"iot:ListThingRegistrationTaskReports",
```

```
    "iot:ListThingRegistrationTasks",
    "iot:ListThings",
    "iot:ListThingsInThingGroup",
    "iot:ListThingTypes",
    "iot:ListTopicRules",
    "iot:ListV2LoggingLevels",
    "iot:SearchIndex",
    "iot:TestAuthorization",
    "iot:TestInvokeAuthorizer",
    "iot:DescribeAccountAuditConfiguration",
    "iot:DescribeAuditTask",
    "iot:ListAuditTasks",
    "iot:DescribeScheduledAudit",
    "iot:ListScheduledAudits",
    "iot:ListAuditFindings",
    "iot:DescribeSecurityProfile",
    "iot:ListSecurityProfiles",
    "iot:ListSecurityProfilesForTarget",
    "iot:ListTargetsForSecurityProfile",
    "iot:ListActiveViolations",
    "iot:ListViolationEvents",
    "iot:ValidateSecurityProfileBehaviors"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDataAccess

AWSIoTDataAccess est une [politique AWS gérée](#) qui : Cette politique donne un accès complet aux actions de messagerie AWS IoT

Utilisation de cette stratégie

Vous pouvez `AWSIoTDataAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 octobre 2015, 21:51 UTC
- Heure modifiée : 23 juin 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot>DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationActionest une [politiqueAWS gérée](#) qui : fournit un accès en écriture aux groupes d'objets IoT et un accès en lecture aux certificats IoT pour l'exécution de l'action d'atténuation ADD_THINGS_TO_THING_GROUP

Utilisation de cette stratégie

Vous pouvez les associerAWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:55 UTC
- Heure modifiée : 7 août 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderAudit

AWSIoTDeviceDefenderAudit est une [politiqueAWS gérée](#) qui : fournit un accès en lecture à l'IoT et aux ressources associées

Utilisation de cette stratégie

Vous pouvez AWSIoTDeviceDefenderAudit les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 18 juillet 2018, 21:17 UTC

- Heure modifiée : 25 novembre 2019, 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction est une [politique AWS gérée](#) qui : Fournit un accès permettant d'activer la journalisation de l'IoT pour l'exécution de l'action d'atténuation ENABLE_IOT_LOGGING

Utilisation de cette stratégie

Vous pouvez AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:04 UTC
- Heure modifiée : 7 août 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction est une [politique AWS gérée](#) qui : fournit aux messages un accès à la rubrique SNS pour l'exécution de l'action d'atténuation PUBLISH_FINDING_TO_SNS

Utilisation de cette stratégie

Vous pouvez les associer AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:04 UTC
- Heure modifiée : 7 août 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction est une [politiqueAWS gérée](#) qui : fournit un accès en écriture aux politiques IoT pour l'exécution de l'action d'atténuation REPLACE_DEFAULT_POLICY_VERSION

Utilisation de cette stratégie

Vous pouvez les associerAWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:04 UTC
- Heure modifiée : 7 août 2019, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction est une [politique AWS gérée](#) qui : fournit un accès en écriture aux certificats IoT CA pour l'exécution de l'action d'atténuation UPDATE_CA_CERTIFICA_CERTIFICATE

Utilisation de cette stratégie

Vous pouvez `AWSIoTDeviceDefenderUpdateCACertMitigationAction` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:05 UTC
- Heure modifiée : 7 août 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

AWSIoTDeviceDefenderUpdateDeviceCertMitigationActionest une [politiqueAWS gérée](#) qui : fournit un accès en écriture aux certificats IoT pour l'exécution de l'action d'atténuation UPDATE_DEVICE_CERTIFICATE

Utilisation de cette stratégie

Vous pouvezAWSIoTDeviceDefenderUpdateDeviceCertMitigationAction les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 août 2019, 17:06 UTC
- Heure modifiée : 7 août 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

AWSIoTDeviceTesterForFreeRTOSFullAccess est un [AWS politique gérée](#) qui : Permet AWS IoT Device Tester exécutera la suite de qualification FreeRTOS en autorisant l'accès à des services tels que l'IoT, S3 et IAM

Utilisation de cette politique

Vous pouvez joindre AWSIoTDeviceTesterForFreeRTOSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 12 février 2020, 20h33 UTC
- Heure modifiée : 10 août 2023, 20h30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Version de la politique

Version de la politique : v7(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
```

```

    "iot:CreateCertificateFromCsr",
    "iot:DetachThingPrincipal",
    "iot:RegisterCACertificate",
    "iot:CreateThing",
    "iam:ListRoles",
    "iot:RegisterCertificate",
    "iot>DeleteCACertificate",
    "signer:PutSigningProfile",
    "s3:ListAllMyBuckets",
    "signer:ListSigningPlatforms",
    "iot-device-tester:SendMetrics",
    "iot-device-tester:SupportedVersion",
    "iot-device-tester:LatestIdt",
    "iot-device-tester:CheckVersion",
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor2",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "signer:StartSigningJob",
    "acm:GetCertificate",
    "signer:DescribeSigningJob",
    "s3:CreateBucket",
    "execute-api:Invoke",
    "s3>DeleteBucket",
    "s3:PutBucketVersioning",
    "signer:CancelSigningProfile"
  ],
  "Resource" : [
    "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
    "arn:aws:signer:*:*/signing-profiles/*",
    "arn:aws:signer:*:*/signing-jobs/*",
    "arn:aws:iam:*:*/role/idt-*",
    "arn:aws:acm:*:*/certificate/*",
    "arn:aws:s3:::idt-*",
    "arn:aws:s3:::afr-ota*"
  ]
},
{
  "Sid" : "VisualEditor3",

```

```

    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteStream",
      "iot:DeleteCertificate",
      "iot:AttachPolicy",
      "iot:DetachPolicy",
      "iot:DeletePolicy",
      "s3:ListBucketVersions",
      "iot:UpdateCertificate",
      "iot:GetOTAUpdate",
      "iot:DeleteOTAUpdate",
      "iot:DescribeJobExecution"
    ],
    "Resource" : [
      "arn:aws:s3:::afr-ota*",
      "arn:aws:iot:*:*:thinggroup/idt*",
      "arn:aws:iam:*:*:role/idt-*"
    ]
  },
  {
    "Sid" : "VisualEditor4",
    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteCertificate",
      "iot:AttachPolicy",
      "iot:DetachPolicy",
      "s3:DeleteObjectVersion",
      "iot:DeleteOTAUpdate",
      "s3:PutObject",
      "s3:GetObject",
      "iot:DeleteStream",
      "iot:DeletePolicy",
      "s3:DeleteObject",
      "iot:UpdateCertificate",
      "iot:GetOTAUpdate",
      "s3:GetObjectVersion",
      "iot:DescribeJobExecution"
    ],
    "Resource" : [
      "arn:aws:s3:::afr-ota*/**",
      "arn:aws:s3:::idt-*/**",
      "arn:aws:iot:*:*:policy/idt*",
      "arn:aws:iam:*:*:role/idt-*",
      "arn:aws:iot:*:*:otaupdate/idt*"
    ]
  }
}

```

```
    "arn:aws:iot:*:*:thing/idt*",
    "arn:aws:iot:*:*:cert/*",
    "arn:aws:iot:*:*:job/*",
    "arn:aws:iot:*:*:stream/*"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::afr-ota/*",
    "arn:aws:s3:::idt-*/*"
  ]
},
{
  "Sid" : "VisualEditor6",
  "Effect" : "Allow",
  "Action" : [
    "iot:CancelJobExecution"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/*",
    "arn:aws:iot:*:*:thing/idt*"
  ]
},
{
  "Sid" : "VisualEditor7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/Owner" : "IoTDeviceTester"
    }
  }
},
},
```

```
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor9",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor10",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:snapshot/*",
```

```

    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "VisualEditor11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ssm:DescribeParameters",
    "ssm:GetParameters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "Owner"
      ]
    }
  }
}

```

```
    ]
  },
  "StringEquals" : {
    "ec2:CreateAction" : [
      "RunInstances",
      "CreateSecurityGroup"
    ]
  }
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWSIoTDeviceTesterForGreengrassFullAccess

AWSIoTDeviceTesterForGreengrassFullAccess est une [politique AWS gérée](#) qui : Permet à AWS IoT Device Tester d'exécuter la suite de qualification AWS Greengrass en autorisant l'accès aux services connexes, notamment Lambda, IoT, API Gateway, IAM

Utilisation de cette stratégie

Vous pouvez AWSIoTDeviceTesterForGreengrassFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 février 2020, 21:21 UTC
- Heure modifiée : 25 juin 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot>DeleteCertificate",
        "lambda>DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda::*:function:idt-*",
        "arn:aws:iot::*:cert/*"
      ]
    }
  ]
}
```

```
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateThing",
    "iot>DeleteThing"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor4",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "iot>DeletePolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
  "Action" : [
    "iot>CreateJob",
    "iot:DescribeJob",
    "iot:DescribeJobExecution",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:job/*"
  ]
},
{
  "Sid" : "VisualEditor6",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iot:DescribeEndpoint",
    "greengrass:*",
    "iam:ListAttachedRolePolicies",
    "iot:CreatePolicy",
    "iot:GetThingShadow",
    "iot:CreateKeysAndCertificate",
    "iot:ListThings",
    "iot:UpdateThingShadow",
    "iot:CreateCertificateFromCsr",
    "iot-device-tester:SendMetrics",
    "iot-device-tester:SupportedVersion",
    "iot-device-tester:LatestIdt",
    "iot-device-tester:CheckVersion",
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor7",
  "Effect" : "Allow",
  "Action" : [
    "iot:DetachThingPrincipal",
    "iot:AttachThingPrincipal"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:DeleteObjectVersion",
    "s3:ListBucketVersions",
    "s3:CreateBucket",
    "s3:DeleteObject",
    "s3:DeleteBucket"
  ],
  "Resource" : "arn:aws:s3:::idt*"
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTEventsFullAccess

AWSIoTEventsFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux IoT Events.

Utilisation de cette stratégie

Vous pouvez AWSIoTEventsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 10 janvier 2019, 22:51 UTC
- Heure modifiée : 10 janvier 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iotevents:*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTEventsReadOnlyAccess

AWSIoTEventsReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux IoT Events.

Utilisation de cette stratégie

Vous pouvez AWSIoTEventsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 10 janvier 2019, 22:50 UTC
- Heure modifiée : 23 septembre 2019, 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoT FleetHub Federation Access

AWSIoT FleetHub Federation Access est une [politique AWS gérée](#) qui : Accès à la fédération pour les applications IoT Fleet Hub

Utilisation de cette stratégie

Vous pouvez AWSIoT FleetHub Federation Access les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 15 décembre 2020, 08:08 UTC
- Heure modifiée : 4 avril 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot>CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot>DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",

```

```
    "iot:ListThingGroups",
    "iot:ListThingsInThingGroup",
    "iot:ListJobTemplates",
    "iot:DescribeJobTemplate",
    "iot:ListJobs",
    "iot:CreateJob",
    "iot:CancelJob",
    "iot:DescribeJob",
    "iot:ListJobExecutionsForJob",
    "iot:ListJobExecutionsForThing",
    "iot:DescribeJobExecution",
    "iot:ListSecurityProfiles",
    "iot:DescribeSecurityProfile",
    "iot:ListActiveViolations",
    "iot:GetThingShadow",
    "iot:ListNamedShadowsForThing",
    "iot:CancelJobExecution",
    "iot:DescribeEndpoint",
    "iotfleethub:DescribeApplication",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:ListSubscriptionsByTopic",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:iotfleethub*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms",
    "cloudwatch:DescribeAlarmHistory"
  ],
}
```



```
    "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoT Fleetwise Service Role Policy

AWSIoT Fleetwise Service Role Policy est une [politiqueAWS gérée](#) qui : accorde des autorisations auxAWS ressources et aux métadonnées utilisées ou gérées par AWSIoT Fleetwise pour les fonctionnalités auxiliaires

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 21 septembre 2022, 23:27 UTC
- Heure modifiée : 21 septembre 2022, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT Fleetwise Service Role Policy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTFullAccess

AWSIoTFullAccess est une [politique AWS gérée](#) qui : Cette politique donne un accès complet à la configuration de l'IoT et aux actions de messagerie

Utilisation de cette stratégie

Vous pouvez AWSIoTFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 octobre 2015, 15:19 UTC
- Heure modifiée : 19 mai 2022, 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTLogging

AWSIoTLogging est une [politique AWS gérée](#) qui : Autorise la création de groupes Amazon CloudWatch Log et la diffusion de journaux vers les groupes

Utilisation de cette stratégie

Vous pouvez AWSIoTLogging les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 8 octobre 2015, 15:17 UTC
- Heure modifiée : 8 octobre 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
      ]
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTOTAUpdate

AWSIoTOTAUpdate est une [politiqueAWS gérée](#) qui : Autorise l'accès à la création d'une JobAWS IoT et à la description de la tâche de signataire deAWS code

Utilisation de cette stratégie

Vous pouvezAWSIoTOTAUpdate les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 décembre 2017, 20:36 UTC
- Heure modifiée : 20 décembre 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTRoboRunnerFullAccess

AWSIoTRoboRunnerFullAccess est une [politiqueAWS gérée](#) qui : Cette politique accorde des autorisations permettant un accès complet àAWS l'IoT RoboRunner.

Utilisation de cette stratégie

Vous pouvezAWSIoTRoboRunnerFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2021, 03:54 UTC
- Heure modifiée : 23 février 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTRoboRunnerReadOnly

`AWSIoTRoboRunnerReadOnly` est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations permettant un accès en lecture seule à AWS IoT RoboRunner.

Utilisation de cette stratégie

Vous pouvez `AWSIoTRoboRunnerReadOnly` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 03:43 UTC
- Heure modifiée : 16 novembre 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",

```



```
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTRoboRunnerServiceRolePolicy

AWSIoTRoboRunnerServiceRolePolicy est une [politique AWS gérée](#) qui : Permet RoboRunner à AWS l'IoT de gérer les AWS ressources associées pour le compte du client.

Utilisation de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

détails des politique

- Type : Politique de rôles liée à un service
- Heure de création : 21 février 2023, 16:56 UTC
- Heure modifiée : 21 février 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document stratégie JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez ez ez ez ez vers les autorisations moindre privilège](#)

AWSIoTRuleActions

AWSIoTRuleAction est une [politique AWS gérée](#) qui : Autorise l'accès à tous les AWS services pris en charge dans AWS IoT Rule Actions

Utilisation de cette stratégie

Vous pouvez AWSIoTRuleActions les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 8 octobre 2015, 15:14 UTC
- Heure modifiée : 16 janvier 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTSiteWiseConsoleFullAccess

AWSIoTSiteWiseConsoleFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à la gestion de SiteWise l'IoT à l'aide duAWS Management Console. Notez que cette politique permet également de créer et de répertorier des magasins de données utilisés avec l'IoT SiteWise (par exemple, AWS IoT Analytics), d'accéder à la liste et à la consultation des ressourcesAWS IoT Greengrass, de répertorier et de modifier lesAWS secrets de Secrets Manager, de récupérer des ombres d'objets de l'IoT, de répertorier les ressources associées à des balises spécifiques, ainsi que de créer et d'utiliser un rôle lié à un service pourAWS l'IoT SiteWise.

Utilisation de cette stratégie

Vous pouvez les associerAWSIoTSiteWiseConsoleFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 31 mai 2019, 21:37 UTC
- Heure modifiée : 31 mai 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : "iotsitewise:*",
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iotanalytics:List*",
      "iotanalytics:Describe*",
      "iotanalytics:Create*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iot:DescribeEndpoint",
      "iot:GetThingShadow"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "greengrass:GetGroup",
      "greengrass:GetGroupVersion",
      "greengrass:GetCoreDefinitionVersion",
      "greengrass:ListGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "secretsmanager:ListSecrets",
      "secretsmanager:CreateSecret"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
```

```

    "secretsmanager:UpdateSecret"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
},
{
  "Action" : [
    "tag:GetResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "iotsitewise.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTSiteWiseFullAccess

AWSIoTSiteWiseFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à l'IoT SiteWise.

Utilisation de cette stratégie

Vous pouvez les associerAWSIoTSiteWiseFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 4 décembre 2018, 20:53 UTC
- Heure modifiée : 4 décembre 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTSiteWiseMonitorPortalAccess

AWSIoTSiteWiseMonitorPortalAccess est une [politique AWS gérée](#) qui : Cette politique autorise l'accès aux SiteWise actifs et aux données des actifs de AWS IoT, à la création de ressources AWS IoT SiteWise Monitor et à la liste des utilisateurs AWS SSO.

Utilisation de cette stratégie

Vous pouvez les associer AWSIoTSiteWiseMonitorPortalAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 19 mai 2020, 20:01 UTC
- Heure modifiée : 19 mai 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise>DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise>DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise>DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
    },
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

AWSIoTSiteWiseMonitorServiceRolePolicy est une [politique AWS gérée](#) qui : Ce rôle accorde à AWS l'IoT des SiteWise autorisations pour accéder à vos SiteWise actifs AWS IoT et à leurs propriétés, et pour créer des projets, des tableaux de bord et des politiques d'accès AWS IoT SiteWise via SiteWise des portails AWS IoT.

Utilisation des stratégies de stratégies de politiques

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, les groupes ou les rôles attachés à des stratégies d'utilisateurs, de groupes ou de rôles attachés

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 14 novembre 2019, 00:59 UTC
- Heure modifiée : 13 décembre 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut d'une stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

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

```
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTSiteWiseReadOnlyAccess

AWSIoTSiteWiseReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à l'IoT SiteWise.

Utilisation de cette stratégie

Vous pouvez les associer AWSIoTSiteWiseReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 4 décembre 2018, 20:55 UTC
- Heure modifiée : 16 septembre 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTThingsRegistration

AWSIoTThingsRegistration est une [politique AWS gérée](#) qui : Cette politique permet aux utilisateurs d'enregistrer des objets en masse à l'aide de l' `StartThingRegistrationTask` API AWS IoT

Utilisation de cette stratégie

Vous pouvez les associer `AWSIoTThingsRegistration` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2017, 20:21 UTC
- Heure modifiée : 5 octobre 2020, 19:20 UTC

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

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
```

```
    "iot:UpdateCertificate",
    "iot:UpdateThing",
    "iot:UpdateThingGroupsForThing",
    "iot:AddThingToBillingGroup",
    "iot:DescribeBillingGroup",
    "iot:RemoveThingFromBillingGroup"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTtwinMakerServiceRolePolicy

AWSIoTtwinMakerServiceRolePolicy est une [politique AWS gérée](#) qui : permet TwinMaker à AWS IoT d'appeler d'autres AWS services et de synchroniser leurs ressources en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 13 novembre 2023, 18:59 UTC
- Heure modifiée : 13 novembre 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```



```
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker>DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker>DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITWISE"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSIoTWirelessDataAccess

AWSIoTWirelessDataAccess est une [politique AWS gérée](#) qui : Autorise l'accès aux données d'identité associées aux appareils AWS IoT Wireless.

Utilisation de cette stratégie

Vous pouvez les associer `AWSIoTWirelessDataAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:31 UTC
- Heure modifiée : 15 décembre 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTWirelessFullAccess

AWSIoTWirelessFullAccess est une [politiqueAWS gérée](#) qui : autorise l'identité associée à un accès complet à toutes les opérationsAWS IoT Wireless.

Utilisation de cette stratégie

Vous pouvezAWSIoTWirelessFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 décembre 2020, 15:27 UTC
- Heure modifiée : 15 décembre 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTWirelessFullPublishAccess

AWSIoTWirelessFullPublishAccess est une [politiqueAWS gérée](#) qui : fournit à IoT Wireless un accès complet pour publier sur IoT Rules Engine en votre nom.

Utilisation de cette stratégie

Vous pouvez AWSIoTWirelessFullPublishAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 décembre 2020, 15:29 UTC
- Heure modifiée : 15 décembre 2020, 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTWirelessGatewayCertManager

AWSIoTWirelessGatewayCertManagerest une [politiqueAWS gérée](#) qui : Autorise l'accès à l'identité associée à la création, à la liste et à la description des certificats IoT

Utilisation de cette stratégie

Vous pouvezAWSIoTWirelessGatewayCertManager les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 décembre 2020, 15h30 UTC

- Heure modifiée : 15 décembre 2020, 15h30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTWirelessLogging

AWSIoTWirelessLogging est une [politique AWS gérée](#) qui : autorise l'identité associée à créer des groupes Amazon CloudWatch Logs et à diffuser des journaux vers ces groupes.

Utilisation de cette stratégie

Vous pouvez les associer AWSIoTWirelessLogging à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:32 UTC
- Heure modifiée : 15 décembre 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIoTWirelessReadOnlyAccess

AWSIoTWirelessReadOnlyAccess est une [politiqueAWS gérée](#) qui : Autorise l'identité associée à un accès en lecture seule àAWS l'IoT sans fil.

Utilisation de cette stratégie

Vous pouvezAWSIoTWirelessReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 15 décembre 2020, 15:28 UTC
- Heure modifiée : 15 décembre 2020, 15:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIPAMServiceRolePolicy

AWSIPAMServiceRolePolicy est une [politique AWS gérée](#) qui : autorise le gestionnaire d'adresses IP VPC à accéder aux ressources du VPC et à s'intégrer aux AWS Organizations en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 30 novembre 2021, 19:08 UTC

- Heure modifiée : 8 novembre 2023, 19:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchMetricsPublishActions",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/IPAM"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy est une [politique AWS gérée](#) qui : Utilisée par AWS IQ pour exécuter les demandes de paiement pour le compte d'un client

utilisation des politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

les détails des politique

- Type : Politique de rôles liée à un service
- Heure de création : 22 août 2019, 19:28 UTC
- Heure modifiée : 22 août 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document des politique JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer les politiques](#)

AWSIQFullAccess

AWSIQFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS IQ

Utilisation de cette stratégie

Vous pouvez AWSIQFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 4 avril 2019, 23:13 UTC
- Heure modifiée : 25 septembre 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSIQPermissionServiceRolePolicy

AWSIQPermissionServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet àAWS IQ de gérer le rôle assumé par les expertsAWS IQ.

Utilisation des de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des utilisateurs, des groupes ou des rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 22 août 2019, 19:36 UTC
- Heure modifiée : 22 août 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version de la stratégie est la version qui définit les autorisations de politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteRole",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DetachRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS de moindre privilège et évoluez vers des autorisations de moindre privilège](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy est une [politique AWS gérée](#) qui : permet l'accès aux AWS services et aux ressources requis pour les magasins de clés personnalisés AWS KMS

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 14 novembre 2018, 20:10 UTC
- Heure modifiée : 10 novembre 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
```



```
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à AWS KMS de synchroniser les propriétés partagées des clés multirégionales.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les utilisateurs.

Utilisation des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 16 juin 2021, 15:37 UTC
- Heure modifiée : 16 juin 2021, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSKeyManagementServicePowerUser

AWSKeyManagementServicePowerUser est une [politique AWS gérée](#) qui : fournit un accès au service de gestion des AWS clés (KMS).

Utilisation de cette stratégie

Vous pouvez AWSKeyManagementServicePowerUser les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 7 mars 2017, 00:55 UTC

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

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms>DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLakeFormationCrossAccountManager

AWSLakeFormationCrossAccountManager est une [politique AWS gérée](#) qui : fournit un accès multicompte aux ressources de Glue via Lake Formation. Accorde également un accès en lecture à d'autres services requis, tels que les organisations et le gestionnaire d'accès aux ressources

Utilisation de cette politique

Vous pouvez vous associer AWSLakeFormationCrossAccountManager à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 août 2020, 20:59 UTC
- Heure modifiée : 1 novembre 2023, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ram:RequestedResourceType" : [
          "glue:Table",
          "glue:Database",
          "glue:Catalog"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ram:UpdateResourceShare",
      "ram>DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:GetResourceShares"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : [
          "LakeFormation*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceSharePermission"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:PermissionArn" : [
          "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        ]
      }
    }
  }
],
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "glue:PutResourcePolicy",
    "glue>DeleteResourcePolicy",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "ram:Get*",
    "ram:List*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListRoots",
    "organizations:ListAccountsForParent",
    "organizations:ListOrganizationalUnitsForParent"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin est une [politique AWS gérée](#) qui : accorde un accès administratif à AWS Lake Formation et aux services connexes, tels que AWS Glue, pour gérer les lacs de données

Utilisation de cette stratégie

Vous pouvez les associer AWSLakeFormationDataAdmin à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 8 août 2019, 17:33 UTC
- Heure modifiée : 16 décembre 2019, 22:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue>DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue>DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",

```

```
    "glue:GetWorkflow",
    "glue:ListWorkflows",
    "glue:BatchGetWorkflows",
    "glue>DeleteWorkflow",
    "glue:GetWorkflowRuns",
    "glue:StartWorkflowRun",
    "glue:GetWorkflow",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "iam:ListUsers",
    "iam:ListRoles",
    "iam:GetRole",
    "iam:GetRolePolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "lakeformation:PutDataLakeSettings"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambda_FullAccess

AWSLambda_FullAccess est une [politique AWS gérée](#) qui : accorde un accès complet au service AWS Lambda, aux fonctionnalités de la console AWS Lambda et à d'autres AWS services connexes.

Utilisation de cette stratégie

Vous pouvez `AWSLambda_FullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 novembre 2020, 21:14 UTC
- Heure modifiée : 17 novembre 2020, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",

```

```
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "lambda:*",
    "logs:DescribeLogGroups",
    "states:DescribeStateMachine",
    "states:ListStateMachines",
    "tag:GetResources",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:FilterLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambda_ReadOnlyAccess

AWSLambda_ReadOnlyAccess est un [AWS Politique gérée](#) qui : Accorde un accès en lecture seule à AWS service Lambda, AWS Fonctionnalités de la console Lambda et autres fonctionnalités connexes AWS services.

Utilisation de cette politique

Vous pouvez joindre AWSLambda_ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS Politique gérée
- Heure de création: 17 novembre 2020, 21h10 UTC
- Heure modifiée : 27 juillet 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",

```

```

    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "kms:ListAliases",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "logs:DescribeLogGroups",
    "lambda:Get*",
    "lambda:List*",
    "states:DescribeStateMachine",
    "states:ListStateMachines",
    "tag:GetResources",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:FilterLogEvents",
    "logs:StartQuery",
    "logs:StopQuery",
    "logs:DescribeQueries",
    "logs:GetLogGroupFields",
    "logs:GetLogRecord",
    "logs:GetQueryResults"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
}

```

En savoir plus

- [Créer un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSLambdaBasicExecutionRole

AWSLambdaBasicExecutionRole est une [politique AWS gérée](#) qui : fournit des autorisations d'écriture dans les CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvez AWSLambdaBasicExecutionRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 avril 2015, 15:03 UTC
- Heure modifiée : 09 avril 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaDynamoDBExecutionRole

AWSLambdaDynamoDBExecutionRoleest une [politiqueAWS gérée](#) qui : fournit un accès en liste et en lecture aux flux DynamoDB et des autorisations d'écriture dans les CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvezAWSLambdaDynamoDBExecutionRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 avril 2015, 15:09 UTC
- Heure modifiée : 09 avril 2015, 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess est une [politiqueAWS gérée](#) qui : fournit des autorisations minimales à une fonction Lambda afin de gérer les ENI (créer, décrire, supprimer) utilisés par une fonction Lambda compatible VPC.

Utilisation de cette stratégie

Vous pouvez AWSLambdaENIManagementAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 décembre 2016, 00:37 UTC
- Heure modifiée : 01 octobre 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS LambdaExecute

AWS LambdaExecute est une [politique AWS gérée](#) qui : fournit un accès Put, Get à S3 et un accès complet aux CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvez AWS LambdaExecute les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/LambdaExecute`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    ],
    "Resource" : "arn:aws:logs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaFullAccess

AWSLambdaFullAccess est une [politique AWS gérée](#) qui : Cette politique est en voie d'obsolescence. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>. Fournit un accès complet à Lambda, S3, DynamoDB, aux CloudWatch métriques et aux journaux.

Utilisation de cette stratégie

Vous pouvez AWSLambdaFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2017, 23:22 UTC

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

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
```

```
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy",
    "iot:CreateThing",
    "iot:CreateTopicRule",
    "iot:DescribeEndpoint",
    "iot:GetTopicRule",
    "iot:ListPolicies",
    "iot:ListThings",
    "iot:ListTopicRules",
    "iot:ReplaceTopicRule",
    "kinesis:DescribeStream",
    "kinesis:ListStreams",
    "kinesis:PutRecord",
    "kms:ListAliases",
    "lambda:*",
    "logs:*",
    "s3:*",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sns:Publish",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sqs:ListQueues",
    "sqs:SendMessage",
    "tag:GetResources",
    "xray:PutTelemetryRecords",
    "xray:PutTraceSegments"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaInvocation-DynamoDB

AWSLambdaInvocation-DynamoDB est une [politique AWS gérée](#) qui : Fournit un accès en lecture aux DynamoDB Streams.

Utilisation de cette stratégie

Vous pouvez AWSLambdaInvocation-DynamoDB les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 6 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Action" : [
      "dynamodb:DescribeStream",
      "dynamodb:GetRecords",
      "dynamodb:GetShardIterator",
      "dynamodb:ListStreams"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaKinesisExecutionRole

AWSLambdaKinesisExecutionRole est une [politique AWS gérée](#) qui : fournit un accès en liste et en lecture aux flux Kinesis et des autorisations d'écriture dans les CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvez AWSLambdaKinesisExecutionRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 avril 2015, 15:14 UTC
- Heure modifiée : 19 novembre 2018, 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaMSKExecutionRole

`AWSLambdaMSKExecutionRole` est une [politique AWS gérée](#) qui : fournit les autorisations requises pour accéder au cluster MSK au sein d'un VPC, gérer les ENI (créer, décrire, supprimer) dans le VPC et écrire des autorisations dans les CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvez les associer `AWSLambdaMSKExecutionRole` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 août 2020, 17:35 UTC
- Heure modifiée : 2 août 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
```



```
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcs",
    "ec2:DeleteNetworkInterface",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS Lambda Replicator

AWS Lambda Replicator est une [politique AWS gérée](#) qui : accorde à Lambda Replicator les autorisations nécessaires pour répliquer les fonctions entre les régions

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 mai 2017, 17:53 UTC
- Heure modifiée : 8 décembre 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
```

```
    "Action" : [
      "cloudfront:ListDistributionsByLambdaFunction"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaRole

AWSLambdaRole est une [politiqueAWS gérée](#) qui : Stratégie par défaut pour le rôle de serviceAWS Lambda.

Utilisation de cette stratégie

Vous pouvez les associerAWSLambdaRole à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaSQSQueueExecutionRole

AWSLambdaSQSQueueExecutionRoleest une [politiqueAWS gérée](#) qui : fournit un accès aux attributs de réception, de suppression de messages et de lecture aux files d'attente SQS, et des autorisations d'écriture dans les CloudWatch journaux.

Utilisation de cette stratégie

Vous pouvezAWSLambdaSQSQueueExecutionRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 14 juin 2018, 21:50 UTC
- Heure modifiée : 14 juin 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole est une [politique AWS gérée](#) qui : fournit des autorisations minimales pour l'exécution d'une fonction Lambda lors de l'accès à une ressource au sein d'un VPC : création, description, suppression d'interfaces réseau et autorisation d'écriture dans les journaux. CloudWatch

Utilisation de cette politique

Vous pouvez vous associer AWSLambdaVPCAccessExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 11 février 2016, 23h15 UTC
- Heure modifiée : 5 janvier 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSLicenseManagerConsumptionPolicy

AWSLicenseManagerConsumptionPolicy est une [politique AWS gérée](#) qui : fournit des autorisations permettant d'accéder aux actions de l'API AWS License Manager requises pour utiliser les licences auxquelles l'utilisateur a droit.

Utilisation de cette stratégie

Vous pouvez AWSLicenseManagerConsumptionPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 août 2021, 23:18 UTC
- Heure modifiée : 11 août 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicyest une [politiqueAWS gérée](#) qui : Permet au serviceAWS License Manager Linux Subscriptions de gérer les ressources en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 20 décembre 2022, 18:54 UTC
- Heure modifiée : 20 décembre 2022, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "organizations:DescribeOrganization",
  "organizations:ListAccounts",
  "organizations:DescribeAccount",
  "organizations:ListChildren",
  "organizations:ListParents",
  "organizations:ListAccountsForParent",
  "organizations:ListRoots",
  "organizations:ListAWSServiceAccessForOrganization",
  "organizations:ListDelegatedAdministrators"
],
"Resource" : [
  "*"
]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy est une [politiqueAWS gérée qui : Politique](#) de rôle du compte principal du serviceAWS License Manager

Utilisation de de de de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, un groupe ou un rôle.

Les détails des des des

- Type : Politique de rôles liée à un service
- Heure de création : 26 novembre 2018, 19:03 UTC
- Heure modifiée : 31 mai 2022, 20:50 UTC

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

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les les des les les des les les les les les les. Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de de de la

```
{
  "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"
            ]
        }
    }
}
}

```

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec des autorisations](#)

AWSLicenseManagerMemberAccountRolePolicy

AWSLicenseManagerMemberAccountRolePolicy est une [politique AWS gérée](#) qui : [Politique](#) de rôle du compte des membres du service AWS License Manager

Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou groupes.

détails

- Type : Politique de rôles liée à un service
- Heure de création : 26 novembre 2018, 19:04 UTC
- Heure modifiée : 15 novembre 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "LicenseManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "license-manager:UpdateLicenseSpecificationsForResource",
      "license-manager:GetLicenseConfiguration"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "SSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListInventoryEntries",
      "ssm:GetInventory",
      "ssm:CreateAssociation",
      "ssm:CreateResourceDataSync",
      "ssm>DeleteResourceDataSync",
      "ssm:ListResourceDataSync",
      "ssm:ListAssociations"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "RAMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ram:AcceptResourceShareInvitation",
      "ram:GetResourceShareInvitations"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez](#)

AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy est une [politiqueAWS gérée qui : Politique](#) de rôle par défaut du serviceAWS License Manager

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 26 novembre 2018, 19:02 UTC
- Heure modifiée : 30 juillet 2021, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut est la version qui définit les autorisations Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "IAMPermissionsForCreatingMemberSLR",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3BucketPermissions1",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-license-manager-service-*"
    ]
  },
  {
    "Sid" : "S3BucketPermissions2",
    "Effect" : "Allow",

```

```
"Action" : [
  "s3:ListAllMyBuckets"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "S3ObjectPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::aws-license-manager-service-*"
  ]
},
{
  "Sid" : "SNSAccountPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:aws-license-manager-service-*"
  ]
},
{
  "Sid" : "SNSTopicPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:DescribeHosts"
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "SSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListInventoryEntries",
      "ssm:GetInventory",
      "ssm:CreateAssociation"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "OrganizationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "LicenseManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "license-manager:GetServiceSettings",
      "license-manager:GetLicense*",
      "license-manager:UpdateLicenseSpecificationsForResource",
      "license-manager:List*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

```
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy est une [politiqueAWS gérée](#) qui : Permet au serviceAWS License Manager User Subscriptions de gérer les ressources en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 30 juillet 2022, 01:17 UTC
- Heure modifiée : 21 novembre 2022, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "DSReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ds:DescribeDirectories",
      "ds:GetAuthorizedApplicationDetails"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SSMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetInventory",
      "ssm:GetCommandInvocation",
      "ssm:ListCommandInvocations",
      "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2ReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2WritePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CreateTags"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:productCode" : [
          "bz0vcy31ooqlzk5tsash4r1lik",
          "d44g89hc0gp9jdzm99rznthpw",
          "77yzkpa7kveely1tt7wnsdwoc"
        ]
      }
    }
  }
]
```

```
    ]
  }
},
"Resource" : [
  "arn:aws:ec2:*:*:instance/*"
]
},
{
  "Sid" : "SSMDocumentExecutionPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript"
  ]
},
{
  "Sid" : "SSMInstanceExecutionPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSM2ServicePolicy

AWSM2ServicePolicy est une [politique AWS gérée](#) qui : Permet à AWS M2 de gérer AWS des ressources en votre nom.

Utilisation des stratégies IAM

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 7 juin 2022, 20:26 UTC
- Heure modifiée : 07 juin 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégies est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégies JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeregisterTargets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/M2"
        ]
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSManagedServices_ContactsServiceRolePolicy

AWSManagedServices_ContactsServiceRolePolicy est une [politiqueAWS gérée](#) qui : Autorise lesAWS Managed Services à lire les valeurs des balises desAWS ressources

Utilisation de stratégies

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 mars 2023, 17:07 UTC
- Heure modifiée : 23 mars 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations de stratégie de politique politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

politique JSON

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


Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 décembre 2022, 23:11 UTC
- Heure modifiée : 19 décembre 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON des politiques

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer des stratégies AWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège et évoluez vers les autorisations de moindre privilège](#)

AWSManagedServices_EventsServiceRolePolicy

AWSManagedServices_EventsServiceRolePolicy est une [politique AWS gérée qui : Politique de AWS Managed Services](#) pour activer la fonctionnalité de traitement d'événements AMS.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 7 février 2023, 18:41 UTC
- Heure modifiée : 07 février 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "events:PutTargets",
    "events:PutRule",
    "events:RemoveTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "events.managedservices.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSManagedServicesDeploymentToolkitPolicy

AWSManagedServicesDeploymentToolkitPolicy est une [politiqueAWS gérée](#) qui :
AutoriseAWS Managed Services à gérer la boîte à outils de déploiement en votre nom.

Utilisation de politiques de politique de politique

Cette politique est attachée à un rôle lié à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 9 juin 2022, 18:33 UTC
- Heure modifiée : 10 mai 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON document de

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
```

```

    "s3:GetObjectVersionAttributes",
    "s3:GetObjectVersionForReplication",
    "s3:GetObjectVersionTagging",
    "s3:GetObjectVersionTorrent",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutBucketAcl",
    "s3:PutBucketLogging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:GetTemplate",
    "cloudformation:GetTemplateSummary",
    "cloudformation:TagResource",
    "cloudformation:UntagResource",
    "cloudformation:UpdateTerminationProtection"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr>DeleteLifecyclePolicy",
    "ecr>DeleteRepository",
    "ecr>DeleteRepositoryPolicy",

```

```
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
    ],
    "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège.](#)

AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion est une [politique AWS gérée](#) qui : Permet AWS Marketplace de copier vos Amazon Machine Images (AMI) afin de les répertorier sur AWS Marketplace

Utilisation de cette stratégie

Vous pouvez AWSMarketplaceAmiIngestion les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 septembre 2020, 20:55 UTC
- Heure modifiée : 25 septembre 2020, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy est une [politique AWS gérée](#) qui : permet de AWS Marketplace créer et de gérer les paramètres de déploiement des vendeurs pour les produits auxquels vous vous abonnez AWS Marketplace.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 15 novembre 2023, 23:34 UTC
- Heure modifiée : 15 novembre 2023, 23h34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
```

```

    "secretsmanager:DeleteSecret",
    "secretsmanager:RemoveRegionsFromReplication"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "ListSecrets",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "TagMarketplaceDeploymentSecrets",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/expirationDate" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "expirationDate"
      ]
    },
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]

```

```
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMarketplaceFullAccess

AWSMarketplaceFullAccess est une [politiqueAWS gérée](#) qui : permet de s'abonner et de se désabonner à desAWS Marketplace logiciels, permet aux utilisateurs de gérer les instances logicielles du Marketplace à partir de la page « Votre logiciel » du Marketplace et fournit un accès administratif à EC2.

Utilisation de cette stratégie

Vous pouvezAWSMarketplaceFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 février 2015, 17:21 UTC
- Heure modifiée : 4 mars 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:*",
    "cloudformation:CreateStack",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:List*",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:CreateTags",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcs",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DeregisterImage",
    "ec2:DescribeSnapshots",
    "ec2>DeleteSnapshot",
    "ec2:CreateImage",
    "ec2:DescribeInstanceStatus",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:DescribeDocument",
    "sns:ListTopics",
```



```
    "sns:GetTopicAttributes",
    "sns:CreateTopic",
    "iam:GetRole",
    "iam:GetInstanceProfile",
    "iam:ListRoles",
    "iam:ListInstanceProfiles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish",
    "sns:setTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:*image-build*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
```

```

    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
      "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
      "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
      "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
      "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
      "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
      "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
      "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ssm.amazonaws.com"
        ],
        "iam:AssociatedResourceARN" : [
          "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
          "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
          "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
          "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
          "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
          "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
          "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
          "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceGetEntitlements

AWSMarketplaceGetEntitlements est une [politiqueAWS gérée](#) qui : Fournit un accès enAWS Marketplace lecture aux autorisations

Utilisation de cette stratégie

Vous pouvezAWSMarketplaceGetEntitlements les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mars 2017, 19:37 UTC
- Heure modifiée : 27 mars 2017, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Action" : [
      "aws-marketplace:GetEntitlements"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à la fonctionnalitéAWS Marketplace Private Image Build. En plus de créer des images privées, il fournit également des autorisations pour ajouter des balises aux images, lancer et fermer des instances ec2.

Utilisation de cette stratégie

Vous pouvezAWSMarketplaceImageBuildFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 31 juillet 2018, 23:29 UTC
- Heure modifiée : 4 mars 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:DescribeDocument",
    "ec2:DeregisterImage",
    "ec2:CopyImage",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2>DeleteSnapshot",
    "ec2:CreateImage",
    "ec2:RunInstances",
    "ec2:DescribeInstanceStatus",
    "sns:GetTopicAttributes",
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3::*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2::*:image/*",
    "arn:aws:ec2::*:instance/*"
  ]
}

```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
    "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
    "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
    "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
    "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
    "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
    "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
    "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ],
      "iam:AssociatedResourceARN" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
```

```
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
    ]
}
},
{
    "Effect" : "Deny",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

AWSMarketplaceLicenseManagementServiceRolePolicy est une [politique AWS gérée](#) qui :
Autorise l'accès Services AWS aux ressources utilisées ou gérées AWS Marketplace pour la gestion des licences.

Utilisation de stratégies Utilisation de stratégies Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, des groupes ou des rôles.

détails des politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 3 décembre 2020, 08:33 UTC
- Heure modifiée : 3 décembre 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie est des stratégies gérées. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document de stratégie JSON, 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" : [
    "*"
  ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez les autorisations gérées et évoluez les autorisations gérées et évoluez les autorisations gérées et évoluez](#)

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions est une [politiqueAWS gérée](#) qui : Permet de s'abonner et de se désabonner à desAWS Marketplace logiciels

Utilisation de cette stratégie

Vous pouvez les associerAWSMarketplaceManageSubscriptions à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 19 janvier 2023, 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceMeteringFullAccess

AWSMarketplaceMeteringFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet auAWS Marketplace comptage.

Utilisation de cette stratégie

Vous pouvezAWSMarketplaceMeteringFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 17 mars 2016, 22:39 UTC
- Heure modifiée : 17 mars 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceMeteringRegisterUsage

AWSMarketplaceMeteringRegisterUsage est une [politique AWS gérée](#) qui : fournit des autorisations pour enregistrer une ressource et suivre son utilisation via AWS Marketplace Metering Service.

Utilisation de cette stratégie

Vous pouvez les associer AWSMarketplaceMeteringRegisterUsage à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 21 novembre 2019, 01:17 UTC
- Heure modifiée : 21 novembre 2019, 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceProcurementSystemAdminFullAccess

AWSMarketplaceProcurementSystemAdminFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les actions administratives nécessaires à une intégration d'AWS Marketplace Procurement.

Utilisation de cette stratégie

Vous pouvez les associer `AWSMarketplaceProcurementSystemAdminFullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 juin 2019, 13:07 UTC
- Heure modifiée : 25 juin 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

AWSMarketplacePurchaseOrdersServiceRolePolicyest une [politiqueAWS gérée](#) qui :
Permet l'accès auxAWS Marketplace services de gestion des bons de commande.

Utilisation des politiques

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom.
Vous ne pouvez pas attacher cette stratégie à vos les les les les les les les les les les les les les les les les les

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 27 octobre 2021, 15:12
- Heure modifiée : 27 octobre 2021, 15:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour les autorisations.
Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer des politiques](#)

AWSMarketplaceRead-only

AWSMarketplaceRead-only est une [politique AWS gérée](#) qui : Permet de consulter les AWS Marketplace abonnements

Utilisation de cette stratégie

Vous pouvez AWSMarketplaceRead-only les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 19 janvier 2023, 23:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow"
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:DescribeBuilds",
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ]
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
```

```
    "Action" : [
      "aws-marketplace:ListPrivateMarketplaceRequests",
      "aws-marketplace:DescribePrivateMarketplaceRequests"
    ],
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:ListPrivateListings"
    ],
    "Resource" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

AWSMarketplaceResaleAuthorizationServiceRolePolicy est une [politique AWS gérée](#) qui : autorise l'accès Services AWS et les ressources utilisées ou gérées par AWS Marketplace pour l'autorisation de revente.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 05 mars 2024, 18:47 UTC
- Heure modifiée : 5 mars 2024, 18:47 UTC

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

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
```

```
    "ram:AssociateResourceShare"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:*"
  ],
  "Condition" : {
    "Null" : {
      "ram:Principal" : "false"
    },
    "StringEquals" : {
      "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
    }
  }
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
  "Effect" : "Allow",
  "Action" : [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
    }
  }
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:*"
  ]
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
  "Effect" : "Allow",
  "Action" : [
```

```
    "aws-marketplace:PutResourcePolicy",
    "aws-marketplace:GetResourcePolicy"
  ],
  "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "ram.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:DescribeEntity"
  ],
  "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMarketplaceSellerFullAccess

AWSMarketplaceSellerFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les opérations du vendeur sur le AWS Marketplace et à d'autres AWS services tels que la gestion des AMI.

Utilisation de cette politique

Vous pouvez vous associer AWSMarketplaceSellerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 2 juillet 2019, 20:40 UTC
- Heure modifiée : 15 mars 2024, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewMarketing",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace-management:viewSettings",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "aws-marketplace:GetSellerDashboard",
      ]
    }
  ]
}
```

```
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots",
    "ec2:ModifyImageAttribute",
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AgreementAccess",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:SearchAgreements",
    "aws-marketplace:DescribeAgreement",
    "aws-marketplace:GetAgreementTerms"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws-marketplace:PartyType" : "Proposer"
    },
    "ForAllValues:StringEquals" : {
      "aws-marketplace:AgreementType" : [
        "PurchaseAgreement"
      ]
    }
  }
},
{
  "Sid" : "IAMGetRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "AssetScanning",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
```



```

        "iam:PassedToService" : "assets.marketplace.amazonaws.com"
    }
}
},
{
    "Sid" : "VendorInsights",
    "Effect" : "Allow",
    "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
    ],
    "Resource" : "*"
},
{
    "Sid" : "TagManagement",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
},
{
    "Sid" : "SellerSettings",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument"
    ]
}

```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Support",
    "Effect" : "Allow",
    "Action" : [
      "support:CreateCase"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ResourcePolicyManagement",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:GetResourcePolicy",
      "aws-marketplace:PutResourcePolicy",
      "aws-marketplace>DeleteResourcePolicy"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMarketplaceSellerProductsFullAccess

AWSMarketplaceSellerProductsFullAccess est un [AWS politique gérée](#) qui : fournit aux vendeurs un accès complet à AWS Marketplace Page des produits de gestion et autres AWS des services tels que la gestion des AMI.

Utilisation de cette politique

Vous pouvez joindre AWSMarketplaceSellerProductsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 2 juillet 2019, 21:06 UTC
- Heure de modification : 18 juillet 2023, 22h19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",

```

```
    "aws-marketplace:DescribeEntity",
    "aws-marketplace:ListTasks",
    "aws-marketplace:DescribeTask",
    "aws-marketplace:UpdateTask",
    "aws-marketplace:CompleteTask",
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots",
    "ec2:ModifyImageAttribute",
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "assets.marketplace.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "vendor-insights:GetDataSource",
    "vendor-insights:ListDataSources",
    "vendor-insights:ListSecurityProfiles",
    "vendor-insights:GetSecurityProfile",
    "vendor-insights:GetSecurityProfileSnapshot",
    "vendor-insights:ListSecurityProfileSnapshots"
  ],
  "Resource" : "*"
},
{
```

```
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:TagResource",
      "aws-marketplace:UntagResource",
      "aws-marketplace:ListTagsForResource"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:GetResourcePolicy",
      "aws-marketplace:PutResourcePolicy",
      "aws-marketplace>DeleteResourcePolicy"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec des politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSMarketplaceSellerProductsReadOnly

AWSMarketplaceSellerProductsReadOnly est une [politique AWS gérée](#) qui : fournit aux vendeurs un accès en lecture seule à AWS Marketplace la page des produits de gestion.

Utilisation de cette stratégie

Vous pouvez associer AWSMarketplaceSellerProductsReadOnly à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 2 juillet 2019, 21:40 UTC
- Heure modifiée : 19 novembre 2022, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy est une [politique AWS gérée](#) qui : La stratégie par défaut qui permet d'accéder Services AWS aux ressources utilisées ou gérées par MediaConnect.

Utilisation des stratégies Utilisation des politiques Utilisation

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, les groupes ou les rôles.

détails des détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 3 avril 2023, 22:11 UTC
- Heure modifiée : 3 avril 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui permet à la stratégie est la version qui définit les détails des politiques. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:UpdateService",
      "ecs>DeleteService",
      "ecs>CreateService",
      "ecs:DescribeServices",
      "ecs:PutAttributes",
      "ecs>DeleteAttributes",
      "ecs:RunTask",
      "ecs>ListTasks",
      "ecs:StartTask",
      "ecs:StopTask",
      "ecs:DescribeTasks",
      "ecs:DescribeContainerInstances",
      "ecs:UpdateContainerInstancesState"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs>CreateCluster",
      "ecs:RegisterTaskDefinition"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:UpdateCluster",
      "ecs:UpdateClusterSettings",
      "ecs>ListAttributes",
      "ecs:DescribeClusters",
      "ecs:DeregisterContainerInstance",
      "ecs>ListContainerInstances"
    ],
    "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
```



```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers vers les détails des politiques gérées et évoluez vers les détails des politiques gérées](#)

AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy est une [politiqueAWS gérée](#) qui : Active l'accès auxAWS ressources utilisées ou gérées par MediaTailor

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 septembre 2021, 22:27 UTC
- Heure modifiée : 17 septembre 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubDiscoveryAccess

AWSMigrationHubDiscoveryAccess est une [politiqueAWS gérée](#) qui : La politique AWSMigrationHubService permet d'appeler AWSApplicationDiscoveryService au nom du client.

Utilisation de cette stratégie

Vous pouvez AWSMigrationHubDiscoveryAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 août 2017, 13h30 UTC
- Heure modifiée : 6 août 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
        "aws:TagKeys" : "aws:migrationhub:source-id"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "dms:AddTagsToResource",
    "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
    ],
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : "aws:migrationhub:source-id"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeInstanceAttribute"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubDMSAccess

AWSMigrationHubDMSAccess est une [politique AWS gérée qui : Politique](#) permettant au Database Migration Service d'assumer un rôle dans le compte du client pour appeler Migration Hub

Utilisation de cette stratégie

Vous pouvez `AWSMigrationHubDMSAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 août 2017, 14h00 UTC
- Heure modifiée : 7 octobre 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",

```

```
    "mgh:NotifyApplicationState",
    "mgh:DescribeApplicationState",
    "mgh:AssociateDiscoveredResource",
    "mgh:DisassociateDiscoveredResource",
    "mgh:ListDiscoveredResources"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
},
{
  "Action" : [
    "mgh:ListMigrationTasks",
    "mgh:GetHomeRegion"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubFullAccess

AWSMigrationHubFullAccess est une [politiqueAWS gérée](#) qui : Politique gérée pour fournir au client un accès au service Migration Hub

Utilisation de cette stratégie

Vous pouvez AWSMigrationHubFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 août 2017, 14:02 UTC

- Heure modifiée : 19 juin 2019, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "migrationhub.amazonaws.com",
          "dmsintegration.migrationhub.amazonaws.com",
          "smsintegration.migrationhub.amazonaws.com"
        ]
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubOrchestratorConsoleFullAccess

AWSMigrationHubOrchestratorConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès limité à AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage

Service et AWS Secrets Manager. Cette politique accorde également un accès complet au service AWS Migration Hub Orchestrator.

Utilisation de cette politique

Vous pouvez vous associer `AWSMigrationHubOrchestratorConsoleFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:26 UTC
- Heure modifiée : 5 décembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MH0",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Sid" : "S3MH0",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::migrationhub-orchestrator-*",
    "arn:aws:s3:::migrationhub-orchestrator-*/*"
  ]
},
{
  "Sid" : "ListSecrets",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Configuration",
  "Effect" : "Allow",
  "Action" : [
    "discovery:DescribeConfigurations",
    "discovery:ListConfigurations",
    "discovery:GetDiscoverySummary"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetHomeRegion",
  "Effect" : "Allow",
  "Action" : [
    "mgh:GetHomeRegion"
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "EC2Describe",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KMS",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMListProfileRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ECS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:ListClusters"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Account",
    "Effect" : "Allow",
    "Action" : [
      "account:ListRegions"
    ],
    "Resource" : "*"
  }
```

```
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy est une [politique AWS gérée](#) qui : Cette politique doit être jointe aux instances migrées vers SAP et MGN afin que notre service puisse orchestrer les instances en téléchargeant des scripts depuis S3 et récupérer des valeurs secrètes au sein de l'instance EC2.

Utilisation de cette stratégie

Vous pouvez `AWSMigrationHubOrchestratorInstanceRolePolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:43 UTC
- Heure modifiée : 20 avril 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3::migrationhub-orchestrator-*",
        "arn:aws:s3::aws-migrationhub-orchestrator-*/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubOrchestratorPlugin

AWSMigrationHubOrchestratorPlugin est une [politique AWS gérée](#) qui : fournit un accès limité à Amazon Simple Storage Service, à AWS Secrets Manager et aux actions liées aux plugins pour AWS Migration Hub Orchestrator.

Utilisation de cette stratégie

Vous pouvez AWSMigrationHubOrchestratorPlugin les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:25 UTC
- Heure modifiée : 20 avril 2022, 02:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/*prod/*/*put-log-data",
        "arn:aws:execute-api:*:*:*/*prod/*/*put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubOrchestratorServiceRolePolicy

AWSMigrationHubOrchestratorServiceRolePolicy est une [politique AWS gérée](#) qui : fournit les autorisations nécessaires à Migration Hub Orchestrator pour migrer et moderniser vos charges de travail sur site

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 20 avril 2022, 02:24 UTC
- Heure modifiée : 4 mars 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ec2LaunchTemplates",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "getHomeRegion",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SSMcommand",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:GetCommandInvocation",
      "ssm:CancelCommand"
    ],
    "Resource" : [
      "arn:aws:ssm:*::document/AWS-RunRemoteScript",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:s3:::aws-migrationhub-orchestrator-*",
      "arn:aws:s3:::migrationhub-orchestrator-*"
    ]
  },
  {

```

```
"Sid" : "SSM",
"Effect" : "Allow",
"Action" : [
  "ssm:DescribeInstanceInformation",
  "ssm:GetCommandInvocation"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "s3GetObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::migrationhub-orchestrator-*",
    "arn:aws:s3:::migrationhub-orchestrator-*/*"
  ]
},
{
  "Sid" : "EventBridge",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:DescribeRule",
    "events>DeleteRule",
    "events:PutRule",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
},
{
  "Sid" : "MGN",
  "Effect" : "Allow",
  "Action" : [
    "mgn:GetReplicationConfiguration",
    "mgn:GetLaunchConfiguration",
    "mgn:StartCutover",
    "mgn:FinalizeCutover",
    "mgn:StartTest",
    "mgn:UpdateReplicationConfiguration",
    "mgn:DescribeSourceServers",
```

```

        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifecycleState"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ec2DescribeImportImage",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImportImageTasks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "s3ListBucket",
    "Effect" : "Allow",
    "Action" : "s3:ListBucket",
    "Resource" : "arn:aws:s3:::*",
    "Condition" : {
      "StringLike" : {
        "s3:prefix" : "migrationhub-orchestrator-vmie-*"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess est un [AWS Politique gérée](#) qui : Accorde un accès complet à AWS Migration Hub, Refactor Spaces et autres AWS services connexes sauf AWS Les groupes de sécurité Transit Gateway et EC2 ne sont pas nécessaires lors de l'utilisation d'environnements sans pont réseau. Cette politique exclut également

les autorisations requises pour AWS Lambda et AWS Gestionnaire d'accès aux ressources, car leur portée peut être réduite en fonction des balises.

Utilisation de cette politique

Vous pouvez joindre `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 3 avril 2023, 20:09 UTC
- Heure de modification : 20 juillet 2023, 15h39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

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

```
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcs",
    "ec2:DescribeTags",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeInternetGateways"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpointServiceConfiguration"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateLoadBalancer"
  ],
}
```

```

    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing>CreateLoadBalancerListeners",
      "elasticloadbalancing>CreateListener",
      "elasticloadbalancing>DeleteListener",
      "elasticloadbalancing>DeleteTargetGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/refactor-spaces:route-id" : [
          "*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteLoadBalancer",
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {

```

```
"Effect" : "Allow",
"Action" : [
  "elasticloadbalancing:AddTags",
  "elasticloadbalancing:CreateListener"
],
"Resource" : [
  "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
  "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
],
"Condition" : {
  "Null" : {
    "aws:RequestTag/refactor-spaces:route-id" : "false"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DeleteTargetGroup",
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
```



```

    "apigateway:GET",
    "apigateway:DELETE",
    "apigateway:PATCH",
    "apigateway:POST",
    "apigateway:PUT",
    "apigateway:UpdateRestApiPolicy"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*",
    "arn:aws:apigateway:*::/tags",
    "arn:aws:apigateway:*::/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : [
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack"
  ],
  "Resource" : "*"
},
{

```

```
"Effect" : "Allow",
"Action" : "iam:CreateServiceLinkedRole",
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec des politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy est une [AWS politique gérée](#) qui : Utilise dans le rôle de service IAM transmis au document SSM Automation AWSRefactorSpaces-CreateResources pour accorder les autorisations nécessaires à l'exécution de l'automatisation. La politique accorde un accès en lecture/écriture aux balises EC2 afin de suivre les progrès de l'automatisation. Lorsque le pont réseau de l'environnement Refactor Spaces est activé, l'automatisation ajoute également le groupe de sécurité de l'environnement à l'instance EC2 pour autoriser le trafic provenant d'autres services Refactor Spaces de l'environnement. La politique donne

également accès aux paramètres SSM des actions post-lancement du service de migration des applications.

Utilisation de cette politique

Vous pouvez joindre `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux rôles de service
- Heure de création: 10 août 2023, 15h08 UTC
- Heure modifiée :10 août 2023, 15 h 08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Version de la politique

Version de la politique : v1(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:ModifyInstanceAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyInstanceAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ssm:GetParameters",
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  }
]
}

```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWS MigrationHubRefactorSpacesFullAccess

`AWSMigrationHubRefactorSpacesFullAccess` est un [AWS politique gérée](#) qui : Accorde un accès complet à AWS MigrationHubRefactor Spaces, AWS MigrationHub Fonctionnalités de la console Refactor Spaces et autres fonctionnalités connexes AWS services à l'exception des autorisations requises pour AWS Lambda et AWS Gestionnaire d'accès aux ressources, car leur portée peut être réduite en fonction des balises.

Utilisation de cette politique

Vous pouvez joindre `AWSMigrationHubRefactorSpacesFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 29 novembre 2021, 07h12 UTC
- Heure de modification : 19 juillet 2023, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTransitGateway",
      "ec2:CreateSecurityGroup",
      "ec2:CreateTransitGatewayVpcAttachment"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:environment-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpointServiceConfiguration"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteTransitGateway",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2>DeleteSecurityGroup",
      "ec2>DeleteTransitGatewayVpcAttachment",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2>DeleteTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:environment-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2>DeleteVpcEndpointServiceConfigurations",
```

```

    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateLoadBalancer"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:CreateLoadBalancerListeners",
      "elasticloadbalancing:CreateListener",
      "elasticloadbalancing>DeleteListener",
      "elasticloadbalancing>DeleteTargetGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {

```



```

        "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
        ]
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DeleteLoadBalancer",
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
        "Null" : {
            "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteListener",
    "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing>DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
},
{
    "Effect" : "Allow",
    "Action" : [

```

```

    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET",
    "apigateway:DELETE",
    "apigateway:PATCH",
    "apigateway:POST",
    "apigateway:PUT",
    "apigateway:UpdateRestApiPolicy"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/restapis/*",
    "arn:aws:apigateway:*:*/vpclinks",
    "arn:aws:apigateway:*:*/vpclinks/*",
    "arn:aws:apigateway:*:*/tags",
    "arn:aws:apigateway:*:*/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : [
    "arn:aws:apigateway:*:*/vpclinks",
    "arn:aws:apigateway:*:*/vpclinks/*"
  ]
},
{
  "Effect" : "Allow",

```

```
    "Action" : [
      "organizations:DescribeOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

AWSMigrationHubRefactorSpacesServiceRolePolicy est un [AWS politique gérée](#) qui : Permet d'accéder à AWS Ressources gérées ou utilisées par AWS Migration Hub Refactor Spaces.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type: Politique des rôles liés au service
- Heure de création: 29 novembre 2021, 06h50 UTC
- Heure modifiée :20 juillet 2023, 15h57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Version de la politique

Version de la politique : v3(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```

    "ec2:DescribeTransitGatewayVpcAttachments",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetGroups",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTransitGatewayVpcAttachment",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2>DeleteTags",
    "ram>DeleteResourceShare",
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2>DeleteVpcEndpointServiceConfigurations",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:CreateLoadBalancerListeners",

```

```

    "elasticloadbalancing:CreateListener",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/refactor-spaces:route-id" : [
        "*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:PUT",
    "apigateway:POST",
    "apigateway:GET",
    "apigateway:PATCH",
    "apigateway:DELETE"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/vpclinks/*",
    "arn:aws:apigateway:*::/tags",
    "arn:aws:apigateway:*::/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteLoadBalancer",

```

```
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
      "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteListener",
    "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing>DeleteTargetGroup",
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DeregisterTargets"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:route-id" : "false"
      }
    }
  }
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
}
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess est une [politique AWS gérée qui : Politique](#) permettant au service de migration des serveurs d'assumer un rôle dans le compte du client pour appeler Migration Hub

Utilisation de cette stratégie

Vous pouvez les associer AWSMigrationHubSMSAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 août 2017, 13:57 UTC
- Heure modifiée : 7 octobre 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh>ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh>ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMigrationHubStrategyCollector

AWSMigrationHubStrategyCollector est une [politique AWS gérée](#) qui : accorde des autorisations pour autoriser la communication avec le service AWS Migration Hub Strategy Recommendations, un accès en lecture/écriture aux compartiments S3 liés au service, un accès Amazon API Gateway pour y télécharger des journaux et des métriques, un accès à AWS Secrets Manager pour récupérer les informations d'identification, et tous les services associés.

Utilisation de cette politique

Vous pouvez vous associer AWSMigrationHubStrategyCollector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 octobre 2021, 20:15 UTC
- Heure modifiée : 5 février 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ],
  {
```

```
"Sid" : "MHSRAllowMetricsAndLogs",
"Effect" : "Allow",
"Action" : [
  "application-transformation:PutMetricData",
  "application-transformation:PutLogData"
],
"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"
  ],
  "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}"
    }
  }
}
```

```
    }  
  }  
} ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSMigrationHubStrategyConsoleFullAccess

AWSMigrationHubStrategyConsoleFullAccess est une [politique AWS gérée](#) qui : accorde un accès complet au service AWS Migration Hub Strategy Recommendations et un accès aux AWS services connexes via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AWSMigrationHubStrategyConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 19 octobre 2021, 20:13 UTC
- Heure modifiée : 09 novembre 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "discovery:GetDiscoverySummary",
    "discovery:DescribeTags",
    "discovery:DescribeConfigurations",
    "discovery:ListConfigurations"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)


```

    "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-*"
  }
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées gérées gérées gérées gérées gérées et évoluez vers les autorisations de moindre privilège gérées et gérées de stratégies gérées de](#)

AWSMobileHub_FullAccess

AWSMobileHub_FullAccess est une [politiqueAWS gérée](#) qui : Cette politique peut être associée à n'importe quel utilisateur, rôle ou groupe, afin d'autoriser les utilisateurs à créer, supprimer et modifier des projets (et leursAWS ressources associées) dansAWS Mobile Hub. Cela inclut également les

autorisations permettant de générer et de télécharger des exemples de code source d'applications mobiles pour chaque projet Mobile Hub.

Utilisation de cette stratégie

Vous pouvez `AWSMobileHub_FullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 5 janvier 2016, 19:56 UTC
- Heure modifiée : 19 décembre 2019, 23h15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
      ]
    }
  ]
}
```

```
    "devicefarm:ScheduleRun",
    "dynamodb:DescribeTable",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "iam:ListSAMLProviders",
    "lambda:ListFunctions",
    "sns:ListTopics",
    "lex:GetIntent",
    "lex:GetIntents",
    "lex:GetSlotType",
    "lex:GetSlotTypes",
    "lex:GetBot",
    "lex:GetBots",
    "lex:GetBotAlias",
    "lex:GetBotAliases",
    "mobilehub:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject"
  ],
  "Resource" : "arn:aws:s3::*-mobilehub-*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3::*-mobilehub-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMobileHub_ReadOnly

AWSMobileHub_ReadOnlyest une [politiqueAWS gérée](#) qui : Cette politique peut être associée à n'importe quel utilisateur, rôle ou groupe, afin d'autoriser les utilisateurs à répertorier et à consulter des projets dansAWS Mobile Hub. Cela inclut également les autorisations permettant de générer et de télécharger des exemples de code source d'applications mobiles pour chaque projet Mobile Hub. Il ne permet pas à l'utilisateur de modifier la configuration d'un projet Mobile Hub.

Utilisation de cette stratégie

Vous pouvezAWSMobileHub_ReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 5 janvier 2016, 19:55 UTC
- Heure modifiée : 23 juillet 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Version de la politique

Version de la politique :v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:DescribeTable",
      "iam:ListSAMLProviders",
      "lambda:ListFunctions",
      "sns:ListTopics",
      "lex:GetIntent",
      "lex:GetIntents",
      "lex:GetSlotType",
      "lex:GetSlotTypes",
      "lex:GetBot",
      "lex:GetBots",
      "lex:GetBotAlias",
      "lex:GetBotAliases",
      "mobilehub:ExportProject",
      "mobilehub:GenerateProjectParameters",
      "mobilehub:GetProject",
      "mobilehub:SynchronizeProject",
      "mobilehub:GetProjectSnapshot",
      "mobilehub:ListProjectSnapshots",
      "mobilehub:ListAvailableConnectors",
      "mobilehub:ListAvailableFeatures",
      "mobilehub:ListAvailableRegions",
      "mobilehub:ListProjects",
      "mobilehub:ValidateProject",
      "mobilehub:VerifyServiceRole",
      "mobilehub:DescribeBundle",
      "mobilehub:ExportBundle",
      "mobilehub:ListBundles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
  }
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSMSKReplicatorExecutionRole

AWSMSKReplicatorExecutionRole est une [politique AWS gérée](#) qui : accorde des autorisations à Amazon MSK Replicator pour répliquer des données entre des clusters MSK.

Utilisation de cette politique

Vous pouvez vous associer AWSMSKReplicatorExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 06 décembre 2023, 00:07 UTC
- Heure modifiée : 6 décembre 2023, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "ClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "kafka-cluster:Connect",
      "kafka-cluster:DescribeCluster",
      "kafka-cluster:AlterCluster",
      "kafka-cluster:DescribeTopic",
      "kafka-cluster:CreateTopic",
      "kafka-cluster:AlterTopic",
      "kafka-cluster:WriteData",
      "kafka-cluster:ReadData",
      "kafka-cluster:AlterGroup",
      "kafka-cluster:DescribeGroup",
      "kafka-cluster:DescribeTopicDynamicConfiguration",
      "kafka-cluster:AlterTopicDynamicConfiguration"
    ],
    "Resource" : [
      "arn:aws:kafka:*:*:cluster/*"
    ]
  },
  {
    "Sid" : "TopicPermissions",
    "Effect" : "Allow",
    "Action" : [
      "kafka-cluster:DescribeTopic",
      "kafka-cluster:CreateTopic",
      "kafka-cluster:AlterTopic",
      "kafka-cluster:WriteData",
      "kafka-cluster:ReadData",
      "kafka-cluster:DescribeTopicDynamicConfiguration",
      "kafka-cluster:AlterTopicDynamicConfiguration",
      "kafka-cluster:AlterCluster"
    ],
    "Resource" : [
      "arn:aws:kafka:*:*:topic/*/*"
    ]
  },
  {
    "Sid" : "GroupPermissions",
    "Effect" : "Allow",
    "Action" : [
```

```
    "kafka-cluster:AlterGroup",
    "kafka-cluster:DescribeGroup"
  ],
  "Resource" : [
    "arn:aws:kafka:*:*:group/*/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSNetworkFirewallServiceRolePolicy

AWSNetworkFirewallServiceRolePolicy est une [politique AWS gérée](#) qui : Permet AWSNetworkFirewall de créer et de gérer les ressources nécessaires à vos pare-feux.

Utilisation de cette politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles attachés à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 novembre 2020, 17:17 UTC
- Heure modifiée : 30 mars 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version par défaut qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "aws:CalledViaLast" : "resource-groups.amazonaws.com"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : "CreateVpcEndpoint",
            "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
    }
}
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy est une [politiqueAWS gérée](#) qui : Autorise NetworkManager l'accès aux ressources associées à votre réseau central

Utilisation

Cette politique est attachée à un rôle lié au service qui permet à ce service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails

- Type : Politique de rôles liée à un service
- Heure de création : 12 juillet 2022, 12:17 UTC
- Heure modifiée : 12 juillet 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers](#)

AWSNetworkManagerFullAccess

AWSNetworkManagerFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon NetworkManager via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezAWSNetworkManagerFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 décembre 2019, 17:37 UTC
- Heure modifiée : 3 décembre 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "networkmanager.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSNetworkManagerReadOnlyAccess

AWSNetworkManagerReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à Amazon NetworkManager via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associer AWSNetworkManagerReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 décembre 2019, 17:35 UTC
- Heure modifiée : 3 décembre 2019, 17:35 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSNetworkManagerServiceRolePolicy

`AWSNetworkManagerServiceRolePolicy` est une [politique AWS gérée](#) qui : Autorise NetworkManager l'accès aux ressources associées à vos réseaux mondiaux


```

    "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" : "*"
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les autorisations de moindreAWS les autorisations de moindre les autorisations de moindre les autorisations de moindre les autorisations](#)

AWSOpsWorks_FullAccess

AWSOpsWorks_FullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet àAWS OpsWorks.

Utilisation de cette stratégie

Vous pouvezAWSOpsWorks_FullAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politiqueAWS gérée

- Heure de création : 22 janvier 2021, 16:29 UTC
- Heure modifiée : 22 janvier 2021, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
  ],
}
```

```
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "opsworks.amazonaws.com"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs est une [politique AWS gérée](#) qui : permet aux OpsWorks instances dont l'intégration CWLogs est activée d'expédier des journaux et de créer les groupes de journaux requis

Utilisation de la présente stratégie

Vous pouvez AWSOpsWorksCloudWatchLogs les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 mars 2017, 17:47 UTC
- Heure modifiée : 30 mars 2017, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksCMInstanceProfileRole

AWSOpsWorksCMInstanceProfileRole est une [politique AWS gérée](#) qui : fournit un accès S3 aux instances lancées par OpsWorks CM.

Utilisation de cette stratégie

Vous pouvez les associer `AWSOpsWorksCMInstanceProfileRole` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 novembre 2016, 09:48 UTC
- Heure modifiée : 23 avril 2021, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:SignalResource"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
```

```
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListMultipartUploadParts",
    "s3:PutObject"
  ],
  "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
  "Effect" : "Allow"
},
{
  "Action" : "acm:GetCertificate",
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Action" : "secretsmanager:GetSecretValue",
  "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
  "Effect" : "Allow"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksCMServiceRole

AWSOpsWorksCMServiceRole est une [politique AWS gérée](#) qui : Politique de rôle de service à utiliser pour créer des serveurs OpsWorks CM.

Utilisation de cette stratégie

Vous pouvez AWSOpsWorksCMServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 24 novembre 2016, 09:49 UTC
- Heure modifiée : 23 avril 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Version de la politique

Version de la politique :v14 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "tag:UntagResources",

```

```
    "tag:TagResources"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation",
    "ssm:ListCommandInvocations",
    "ssm:ListCommands"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
    }
  },
  "Action" : [
    "ssm:SendCommand"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:ssm:*::document/*",
    "arn:aws:s3:::aws-opsworks-cm-*"
  ],
  "Action" : [
    "ssm:SendCommand"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
}
```

```

    "Action" : [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateImage",
      "ec2:CreateSecurityGroup",
      "ec2:CreateSnapshot",
      "ec2:CreateTags",
      "ec2>DeleteSecurityGroup",
      "ec2>DeleteSnapshot",
      "ec2:DeregisterImage",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress",
      "ec2:RunInstances",
      "ec2:StopInstances"
    ]
  },
  {
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
      }
    },
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:RebootInstances"
    ]
  },
  {
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:opsworks-cm:*:*:server/*"
    ]
  }
}

```



```

    ],
    "Action" : [
        "opsworks-cm:DeleteServer",
        "opsworks-cm:StartMaintenance"
    ]
},
{
    "Effect" : "Allow",
    "Resource" : [
        "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
    ],
    "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack"
    ]
},
{
    "Effect" : "Allow",
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-opsworks-cm-*",
        "arn:aws:iam:*:*:role/service-role/aws-opsworks-cm-*"
    ],
    "Action" : [
        "iam:PassRole"
    ]
},
{
    "Effect" : "Allow",
    "Resource" : "*",
    "Action" : [
        "acm:DeleteCertificate",
        "acm:ImportCertificate"
    ]
},
{
    "Effect" : "Allow",
    "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
    "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",

```

```
        "secretsmanager:UpdateSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "ec2:DeleteTags",
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:security-group/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksInstanceRegistration

AWSOpsWorksInstanceRegistration est une [politiqueAWS gérée](#) qui : permet à une instance Amazon EC2 de s'enregistrer auprès d'uneAWS OpsWorks pile.

Utilisation de cette stratégie

Vous pouvez les associerAWSOpsWorksInstanceRegistration à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 3 juin 2016, 14:23 UTC

- Heure modifiée : 3 juin 2016, 14:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksRegisterCLI_EC2

AWSOpsWorksRegisterCLI_EC2 est une [politique AWS gérée](#) qui : Politique permettant l'enregistrement des instances EC2 via la OpsWorks CLI

Utilisation de cette stratégie

Vous pouvez AWSOpsWorksRegisterCLI_EC2 les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 18 juin 2019, 15:56 UTC
- Heure modifiée : 18 juin 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
```

```
    "opsworks:UnassignInstance"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOpsWorksRegisterCLI_OnPremises

AWSOpsWorksRegisterCLI_OnPremises est une [politiqueAWS gérée](#) qui : Politique permettant l'enregistrement d'instances sur site via l' OpsWorks interface de ligne de commande

Utilisation de cette stratégie

Vous pouvez les associer AWSOpsWorksRegisterCLI_OnPremises à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la stratégie

- Type : politiqueAWS gérée
- Heure de création : 18 juin 2019, 15:33 UTC

- Heure modifiée : 18 juin 2019, 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  {
```

```

    "Effect" : "Allow",
    "Action" : [
      "iam:CreateGroup",
      "iam:AddUserToGroup"
    ],
    "Resource" : [
      "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateUser",
      "iam:CreateAccessKey"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachUserPolicy"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ],
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOrganizationsFullAccess

AWSOrganizationsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux AWS Organisations.

Utilisation de cette politique

Vous pouvez vous associer AWSOrganizationsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 novembre 2018, 20:31 UTC
- Heure modifiée : 6 février 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
```



```
    "account:DeleteAlternateContact",
    "account:GetAlternateContact",
    "account:GetContactInformation",
    "account:PutContactInformation",
    "account:ListRegions",
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSOrganizationsFullAccessCreateSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "organizations.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSOrganizationsReadOnlyAccess

AWSOrganizationsReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux Organisations AWS .

Utilisation de cette politique

Vous pouvez vous associer AWSOrganizationsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 novembre 2018, 20:32 UTC
- Heure modifiée : 6 février 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSOrganizationsServiceTrustPolicy

AWSOrganizationsServiceTrustPolicy est une [politique AWS gérée](#) qui : Une politique permettant aux AWS Organizations de partager la confiance avec d'autres entités approuvées Services AWS dans le but de simplifier la configuration des clients.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 10 octobre 2017, 23:04 UTC
- Heure modifiée : 01 novembre 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JAM

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations vous permettant d'installer un serveur Outpost sur votre réseau local.

Utilisation de cette stratégie

Vous pouvez AWSOutpostsAuthorizeServerPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 4 janvier 2023, 19:23 UTC
- Heure modifiée : 4 janvier 2023, 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSOutpostsServiceRolePolicy

AWSOutpostsServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de rôle lié aux services pour permettre l'accès aux AWS ressources gérées par AWS Outposts

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 09 novembre 2020, 22:55 UTC
- Heure modifiée : 09 novembre 2020, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ]
    }
  ],
}
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaApplianceRolePolicy

AWSPanoramaApplianceRolePolicy est une [politiqueAWS gérée](#) qui : autorise le logicielAWS IoT d'une applianceAWS Panorama à télécharger des journaux sur Amazon CloudWatch.

Utilisation de cette stratégie

Vous pouvezAWSPanoramaApplianceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2020, 13:13 UTC
- Heure modifiée : 01 décembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "PanoramaDeviceCreateLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
  },
  {
    "Sid" : "PanoramaDeviceCreateLogGroup",
    "Effect" : "Allow",
    "Action" : "logs:CreateLogGroup",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaApplianceServiceRolePolicy

AWSPanoramaApplianceServiceRolePolicy est une [politique AWS gérée](#) qui : permet à une appliance AWS Panorama de télécharger des journaux sur Amazon CloudWatch et d'obtenir des objets à partir des points d'accès Amazon S3 créés pour être utilisés avec AWS Panorama.

Utilisation de cette stratégie

Vous pouvez AWSPanoramaApplianceServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 octobre 2021, 12:14 UTC
- Heure modifiée : 17 janvier 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",

```

```
    "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
  ]
},
{
  "Sid" : "PanoramaDevicePutMetric",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "PanoramaDeviceMetrics"
    }
  }
},
{
  "Sid" : "PanoramaDeviceS3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:GetObjectVersion"
  ],
  "Resource" : [
    "arn:aws:s3::*-nodepackage-store-*",
    "arn:aws:s3::*-application-payload-store-*",
    "arn:aws:s3:*:*:accesspoint/panorama*"
  ],
  "Condition" : {
    "StringLike" : {
      "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaFullAccess

AWSPanoramaFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à AWS Panorama

Utilisation de cette stratégie

Vous pouvez AWSPanoramaFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 décembre 2020, 13:12 UTC
- Heure modifiée : 12 janvier 2022, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "s3:PutObjectAcl",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:PutSecretValue",
    "secretsmanager:UpdateSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:panorama*",
    "arn:aws:secretsmanager:*:*:secret:Panorama*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "panorama.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:Describe*",
    "logs:Get*",
    "logs:List*",

```

```
    "logs:StartQuery",
    "logs:StopQuery",
    "logs:TestMetricFilter",
    "logs:FilterLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:ListRoles",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "panorama.amazonaws.com"
    }
  }
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaGreengrassGroupRolePolicy

AWSPanoramaGreengrassGroupRolePolicyest une [politiqueAWS gérée](#) qui : autorise une fonctionAWS Lambda d'une applianceAWS Panorama à gérer les ressources dans Panorama, à télécharger des journaux et des métriques sur Amazon CloudWatch et à gérer des objets dans des compartiments créés pour être utilisés avec Panorama.

Utilisation de cette stratégie

Vous pouvezAWSPanoramaGreengrassGroupRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2020, 13:10 UTC
- Heure modifiée : 6 janvier 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    }
  ],
}
```

```
{
  "Sid" : "PanoramaAccess",
  "Effect" : "Allow",
  "Action" : [
    "panorama:*"
  ],
  "Resource" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicyest une [politiqueAWS gérée](#) qui : Permet SageMaker à Amazon de gérer des objets dans des compartiments créés pour être utilisés avecAWS Panorama.

Utilisation de cette stratégie

Vous pouvezAWSPanoramaSageMakerRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2020, 13:13 UTC
- Heure modifiée : 01 décembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaServiceLinkedRolePolicy

AWSPanoramaServiceLinkedRolePolicyest une [politiqueAWS gérée](#) qui : Permet àAWS Panorama de gérer les ressources dansAWS IoT,AWS Secrets Manager etAWS Panorama.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 20 octobre 2021, 12:12 UTC
- Heure modifiée : 20 octobre 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    }
  ]
}
```

```
]
},
{
  "Sid" : "PanoramaIoTCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal",
    "iot:UpdateCertificate",
    "iot>DeleteCertificate",
    "iot:AttachPrincipalPolicy",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "PanoramaIoTCreateCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion",
    "iot:AttachPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTJobAccess",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iot:DescribeJobExecution",
    "iot:CreateJob",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/panorama*",
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTEndpointAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeEndpoint"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "panorama:Describe*",
    "panorama:List*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "SecretsManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:CreateSecret",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager>DeleteSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:panorama*",
    "arn:aws:secretsmanager:*:*:secret:Panorama*"
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège](#)

AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy est une [politique AWS gérée](#) qui : permet à AWS Panorama de gérer les ressources dans Amazon S3, AWS IoT, AWS Lambda GreenGrass, Amazon et Amazon CloudWatch Logs SageMaker, et de transmettre des rôles de service à AWS IoT, à AWS IoT GreenGrass et à Amazon SageMaker.

Utilisation de cette stratégie

Vous pouvez AWSPanoramaServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 1 décembre 2020, 13:14 UTC
- Heure modifiée : 01 décembre 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot>DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreatePolicyVersion"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:policy/panorama*"
    ]
  },
  {
    "Sid" : "PanoramaIoTJobAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeJobExecution",
      "iot:CreateJob",
      "iot>DeleteJob"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:job/panorama*",
      "arn:aws:iot:*:*:thing/panorama*"
    ]
  },
  {
    "Sid" : "PanoramaIoTEndpointAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeEndpoint"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "PanoramaAccess",
    "Effect" : "Allow",
    "Action" : [
      "panorama:Describe*",
      "panorama:List*",
```

```

    "panorama:Get*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaS3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:DeleteBucket",
    "s3:ListBucket",
    "s3:GetBucket*",
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3::*aws-panorama*"
  ]
},
{
  "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*role/AWSPanoramaSageMakerRole",
    "arn:aws:iam::*role/service-role/AWSPanoramaSageMakerRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
  "Effect" : "Allow",
  "Action" : [

```



```

    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
    "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "greengrass.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "PanoramaIAMPassIoTRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "iot.amazonaws.com"
    }
  }
},
{
  "Sid" : "PanoramaGreenGrassAccess",
  "Effect" : "Allow",
  "Action" : [
    "greengrass:AssociateRoleToGroup",
    "greengrass:AssociateServiceRoleToAccount",
    "greengrass>CreateResourceDefinition",
    "greengrass>CreateResourceDefinitionVersion",
    "greengrass>CreateCoreDefinition",
    "greengrass>CreateCoreDefinitionVersion",
    "greengrass>CreateDeployment",
    "greengrass>CreateFunctionDefinition",

```

```
"greengrass:CreateFunctionDefinitionVersion",
"greengrass:CreateGroup",
"greengrass:CreateGroupCertificateAuthority",
"greengrass:CreateGroupVersion",
"greengrass:CreateLoggerDefinition",
"greengrass:CreateLoggerDefinitionVersion",
"greengrass:CreateSubscriptionDefinition",
"greengrass:CreateSubscriptionDefinitionVersion",
"greengrass>DeleteCoreDefinition",
"greengrass>DeleteFunctionDefinition",
"greengrass>DeleteResourceDefinition",
"greengrass>DeleteGroup",
"greengrass>DeleteLoggerDefinition",
"greengrass>DeleteSubscriptionDefinition",
"greengrass:DisassociateRoleFromGroup",
"greengrass:DisassociateServiceRoleFromAccount",
"greengrass:GetAssociatedRole",
"greengrass:GetConnectivityInfo",
"greengrass:GetCoreDefinition",
"greengrass:GetCoreDefinitionVersion",
"greengrass:GetDeploymentStatus",
"greengrass:GetDeviceDefinition",
"greengrass:GetDeviceDefinitionVersion",
"greengrass:GetFunctionDefinition",
"greengrass:GetFunctionDefinitionVersion",
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
```

```

    "greengrass:ListGroup",
    "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*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPriceListServiceFullAccess

AWSPriceListServiceFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet au serviceAWS Price List.

Utilisation de cette stratégie

Vous pouvezAWSPriceListServiceFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 22 novembre 2017, 00:36 UTC
- Heure modifiée : 22 novembre 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPRivateCAAuditor

AWSPRivateCAAuditor est une [politiqueAWS gérée](#) qui : Fournit à l'auditeur un accès àAWS une autorité de certification privée

Utilisation de cette stratégie

Vous pouvezAWSPRivateCAAuditor les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 février 2023, 18:33 UTC
- Heure modifiée : 14 février 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAAuditor`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:CreateCertificateAuthorityAuditReport",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPriateCAFullAccess

AWSPriateCAFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à l'autorité de certification AWS privée

Utilisation de cette stratégie

Vous pouvez `AWSPrivateCAFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:20 UTC
- Heure modifiée : 14 février 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPrivateCAPrivilegedUser

AWSPrivateCAPrivilegedUserest une [politiqueAWS gérée](#) qui : Fournit aux utilisateurs de certificats privilégiés un accès àAWS une autorité de certification privée

Utilisation de cette stratégie

Vous pouvez les associerAWSPrivateCAPrivilegedUser à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 février 2023, 18:26 UTC
- Heure modifiée : 14 février 2023, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
```

```

    "StringLike" : {
      "acm-pca:TemplateArn" : [
        "arn:aws:acm-pca:::template/*CACertificate*/V*"
      ]
    }
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition" : {
      "StringNotLike" : {
        "acm-pca:TemplateArn" : [
          "arn:aws:acm-pca:::template/*CACertificate*/V*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:RevokeCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:ListPermissions"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPRivateCAReADOnly

AWSPRivateCAReADOnly est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à l'autorité de certificationAWS privée

Utilisation de cette stratégie

Vous pouvezAWSPRivateCAReADOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 février 2023, 18h30 UTC
- Heure modifiée : 14 février 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAReADOnly`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
    ]
  }
}
```

```
    "acm-pca:GetCertificateAuthorityCsr",
    "acm-pca:GetCertificateAuthorityCertificate",
    "acm-pca:GetCertificate",
    "acm-pca:GetPolicy",
    "acm-pca:ListPermissions",
    "acm-pca:ListTags"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPRivateCAUser

AWSPRivateCAUser est une [politiqueAWS gérée](#) qui : Fournit aux utilisateurs de certificats un accès àAWS une autorité de certification privée

Utilisation de cette stratégie

Vous pouvezAWSPRivateCAUser les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 février 2023, 18:16 UTC
- Heure modifiée : 14 février 2023, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPRivateCAUser

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à toutes les actions administratives d'une Marketplace AWS privée.

Utilisation de cette politique

Vous pouvez vous associer AWSPrivateMarketplaceAdminFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 16:32 UTC
- Heure modifiée : 14 février 2024, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
    "aws-marketplace:TagResource",
    "aws-marketplace:UntagResource",
    "aws-marketplace:ListTagsForResource"
  ],
  "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
},
{
  "Sid" : "PrivateMarketplaceOrganizationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAccountsForParent",
    "organizations:ListAccounts",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSPivateMarketplaceRequests

AWSPivateMarketplaceRequests est une [politique AWS gérée](#) qui : Fournit l'accès à la création de demandes sur un Marketplace AWS privé.

Utilisation de cette stratégie

Vous pouvez `AWSPrivateMarketplaceRequests` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 octobre 2019, 21:44 UTC
- Heure modifiée : 28 octobre 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSPrivateNetworksServiceRolePolicy

AWSPrivateNetworksServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise AWS Private Networks Service à gérer les ressources pour le compte du client.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 16 décembre 2021, 23:17 UTC
- Heure modifiée : 16 décembre 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/Private5G"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonCodeBuildProvisioningBasicAccess

AWSProtonCodeBuildProvisioningBasicAccess est une [politiqueAWS gérée](#) qui : Les autorisations CodeBuild doivent exécuter une version pourAWS Proton CodeBuild Provisioning.

Utilisation de cette stratégie

Vous pouvez les associerAWSProtonCodeBuildProvisioningBasicAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 novembre 2022, 21:04 UTC
- Heure modifiée : 09 novembre 2022, 21:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

AWSProtonCodeBuildProvisioningServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à AWS Proton de gérer le provisionnement des ressources ProtonCodeBuild en utilisant d'autres AWS services en votre nom.

Utilisation de politique de politique de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles des politiques de politique de politique de politique de politique de

Détails des politiques de politique

- Type : Politique de rôles liée à un service
- Heure de création : 9 novembre 2022, 21:32 UTC
- Heure modifiée : 17 mai 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de politique est la version qui définit les autorisations de politique par défaut. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON Document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées gérées et évoluez vers les politiques de politiques de politiques de politiques de politiques de politiques de politiques](#)

AWSProtonDeveloperAccess

`AWSProtonDeveloperAccess` est une [politiqueAWS gérée](#) qui : fournit un accès aux API et à la console de gestionAWS Proton, mais n'autorise pas l'administration de modèles ou d'environnements Proton.

Utilisation de cette stratégie

Vous pouvez `AWSProtonDeveloperAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 17 février 2021, 19:02 UTC
- Heure modifiée : 18 novembre 2022, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Action" : [  
  "codecommit:ListRepositories",  
  "codepipeline:GetPipeline",  
  "codepipeline:GetPipelineExecution",  
  "codepipeline:GetPipelineState",  
  "codepipeline:ListPipelineExecutions",  
  "codepipeline:ListPipelines",  
  "codestar-connections:ListConnections",  
  "codestar-connections:UseConnection",  
  "proton:CancelServiceInstanceDeployment",  
  "proton:CancelServicePipelineDeployment",  
  "proton:CreateService",  
  "proton>DeleteService",  
  "proton:GetAccountRoles",  
  "proton:GetAccountSettings",  
  "proton:GetEnvironment",  
  "proton:GetEnvironmentAccountConnection",  
  "proton:GetEnvironmentTemplate",  
  "proton:GetEnvironmentTemplateMajorVersion",  
  "proton:GetEnvironmentTemplateMinorVersion",  
  "proton:GetEnvironmentTemplateVersion",  
  "proton:GetRepository",  
  "proton:GetRepositorySyncStatus",  
  "proton:GetResourcesSummary",  
  "proton:GetService",  
  "proton:GetServiceInstance",  
  "proton:GetServiceTemplate",  
  "proton:GetServiceTemplateMajorVersion",  
  "proton:GetServiceTemplateMinorVersion",  
  "proton:GetServiceTemplateVersion",  
  "proton:GetTemplateSyncConfig",  
  "proton:GetTemplateSyncStatus",  
  "proton:ListEnvironmentAccountConnections",  
  "proton:ListEnvironmentOutputs",  
  "proton:ListEnvironmentProvisionedResources",  
  "proton:ListEnvironments",  
  "proton:ListEnvironmentTemplateMajorVersions",  
  "proton:ListEnvironmentTemplateMinorVersions",  
  "proton:ListEnvironmentTemplates",  
  "proton:ListEnvironmentTemplateVersions",  
  "proton:ListRepositories",  
  "proton:ListRepositorySyncDefinitions",  
  "proton:ListServiceInstanceOutputs",  
  "proton:ListServiceInstanceProvisionedResources",
```



```

    "proton:ListServiceInstances",
    "proton:ListServicePipelineOutputs",
    "proton:ListServicePipelineProvisionedResources",
    "proton:ListServices",
    "proton:ListServiceTemplateMajorVersions",
    "proton:ListServiceTemplateMinorVersions",
    "proton:ListServiceTemplates",
    "proton:ListServiceTemplateVersions",
    "proton:ListTagsForResource",
    "proton:UpdateService",
    "proton:UpdateServiceInstance",
    "proton:UpdateServicePipeline",
    "s3:ListAllMyBuckets",
    "s3:ListBucket"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
  "Condition" : {
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonFullAccess

AWSProtonFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet aux API et à la console de gestionAWS Proton. Outre ces autorisations, l'accès à Amazon S3 est également nécessaire pour enregistrer des ensembles de modèles à partir de vos compartiments S3, ainsi que l'accès à Amazon IAM pour créer et gérer les rôles de service pour Proton.

Utilisation de cette stratégie

Vous pouvez les associerAWSProtonFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 17 février 2021, 19:07 UTC
- Heure modifiée : 20 juin 2022, 12:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "proton.*.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "proton.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/AWSServiceRoleForProtonSync",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "sync.proton.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:PassConnection"
    ],
    "Resource" : "arn:aws:codestar-connections::*:connection/*",
    "Condition" : {
```

```
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonReadOnlyAccess

AWSProtonReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule aux API et à la console de gestionAWS Proton.

Utilisation de cette stratégie

Vous pouvezAWSProtonReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 17 février 2021, 19:09 UTC
- Heure modifiée : 18 novembre 2022, 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",

```

```
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListRepositories",
    "proton:ListRepositorySyncDefinitions",
    "proton:ListServiceInstanceOutputs",
    "proton:ListServiceInstanceProvisionedResources",
    "proton:ListServiceInstances",
    "proton:ListServicePipelineOutputs",
    "proton:ListServicePipelineProvisionedResources",
    "proton:ListServices",
    "proton:ListServiceTemplateMajorVersions",
    "proton:ListServiceTemplateMinorVersions",
    "proton:ListServiceTemplates",
    "proton:ListServiceTemplateVersions",
    "proton:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonServiceGitSyncServiceRolePolicy

AWSProtonServiceGitSyncServiceRolePolicy est une [politique AWS gérée](#) qui : Politique qui permet à AWS Proton de synchroniser vos définitions de service, d'environnement et de composants depuis votre référentiel git vers AWS Proton.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 avril 2023, 15:55 UTC
- Heure modifiée : 4 avril 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ]
    }
  ]
}
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy est une [politiqueAWS gérée qui : Politique](#) qui permet àAWS Proton de synchroniser le contenu de votre dépôt git avec Proton ou de synchroniser le contenu de Proton avec vos référentiels git.

Utilisation des stratégies politiques des stratégies

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos groupes, les groupes, les groupes.

Utilisation des politiques des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 novembre 2021, 21:14 UTC
- Heure modifiée : 23 novembre 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégies est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégies JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton>DeleteServiceTemplateVersion",
        "proton>DeleteEnvironmentTemplateVersion",
        "proton>CreateServiceTemplateVersion",
        "proton>CreateServiceTemplate",
        "proton>CreateEnvironmentTemplateVersion",
        "proton>CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton>CreateEnvironmentTemplateMajorVersion",
        "proton>CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et les politiques gérées et les autorisations de moindre privilège](#)

AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy est un [AWS politique gérée](#) qui : accorde l'autorisation de consulter et de modifier les bons de commande sur la console de facturation

Utilisation de cette politique

Vous pouvez joindre AWSPurchaseOrdersServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 6 mai 2020, 18h15 UTC
- Heure modifiée : 17 juillet 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "account:GetAccountInformation",
  "account:GetContactInformation",
  "aws-portal:*Billing",
  "consolidatedbilling:GetAccountBillingRole",
  "invoicing:GetInvoicePDF",
  "payments:GetPaymentInstrument",
  "payments:ListPaymentPreferences",
  "purchase-orders:AddPurchaseOrder",
  "purchase-orders>DeletePurchaseOrder",
  "purchase-orders:GetPurchaseOrder",
  "purchase-orders:ListPurchaseOrderInvoices",
  "purchase-orders:ListPurchaseOrders",
  "purchase-orders:ListTagsForResource",
  "purchase-orders:ModifyPurchaseOrders",
  "purchase-orders:TagResource",
  "purchase-orders:UntagResource",
  "purchase-orders:UpdatePurchaseOrder",
  "purchase-orders:UpdatePurchaseOrderStatus",
  "purchase-orders:ViewPurchaseOrders",
  "tax:ListTaxRegistrations"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations de moindre privilège](#)

AWSQuicksightAthenaAccess

AWSQuicksightAthenaAccess est une [politiqueAWS gérée](#) qui : Accès rapide à l'API Athena et aux compartiments S3 utilisés pour les résultats des requêtes Athena

Utilisation de cette stratégie

Vous pouvez `AWSQuicksightAthenaAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 9 décembre 2016, 02:31 UTC
- Heure modifiée : 07 juillet 2021, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Version de la politique

Version de la politique :v10 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",

```

```

    "athena:ListQueryExecutions",
    "athena:RunQuery",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution",
    "athena:ListWorkGroups",
    "athena:ListEngineVersions",
    "athena:GetWorkGroup",
    "athena:GetDataCatalog",
    "athena:GetDatabase",
    "athena:GetTableMetadata",
    "athena:ListDataCatalogs",
    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:UpdateDatabase",
    "glue:CreateTable",
    "glue>DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue:GetTable",
    "glue:GetTables",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue>DeletePartition",
    "glue:BatchDeletePartition",
    "glue:UpdatePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchGetPartition"
  ],
  "Resource" : [
    "*"
  ]
}

```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightDescribeRDS

AWSQuickSightDescribeRDS est une [politique AWS gérée](#) qui : Autorise QuickSight à décrire les ressources RDS

Utilisation de cette stratégie

Vous pouvez AWSQuickSightDescribeRDS les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 10 novembre 2015, 23:24 UTC
- Heure modifiée : 10 novembre 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightDescribeRedshift

AWSQuickSightDescribeRedshift est une [politiqueAWS gérée](#) qui : Autorise QuickSight à décrire les ressources Redshift

Utilisation de cette stratégie

Vous pouvez AWSQuickSightDescribeRedshift les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 10 novembre 2015, 23:25 UTC
- Heure modifiée : 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
    "Action" : [
      "redshift:Describe*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy est une [politique AWS gérée](#) qui : Fournit un accès aux ressources Amazon Elasticsearch depuis Amazon QuickSight

Utilisation de cette stratégie

Vous pouvez AWSQuickSightElasticsearchPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 09 septembre 2020, 17:27 UTC
- Heure modifiée : 7 septembre 2021, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",

```

```
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightIoTAnalyticsAccess

AWSQuickSightIoTAnalyticsAccess est une [politique AWS gérée](#) qui : accorde un accès en QuickSight lecture seule aux ensembles de données IoT Analytics

Utilisation de cette stratégie

Vous pouvez AWSQuickSightIoTAnalyticsAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 17h00 UTC
- Heure modifiée : 29 novembre 2017, 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightListIAM

AWSQuickSightListIAMest une [politiqueAWS gérée](#) qui : Autorise QuickSight à répertorier les entités IAM

Utilisation de cette stratégie

Vous pouvez les associerAWSQuickSightListIAM à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 10 novembre 2015, 23:25 UTC

- Heure modifiée : 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuicksightOpenSearchPolicy

AWSQuicksightOpenSearchPolicy est une [politique AWS gérée](#) qui : Fournit un accès aux OpenSearch ressources Amazon depuis Amazon QuickSight

Utilisation de cette stratégie

Vous pouvez les associer `AWSQuicksightOpenSearchPolicy` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 7 septembre 2021, 23:26 UTC
- Heure modifiée : 7 septembre 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "es:DescribeDomain"
    ],
    "Resource" : [
      "arn:aws:es:*:*:domain/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "es:ESHttpPost",
      "es:ESHttpGet"
    ],
    "Resource" : [
      "arn:aws:es:*:*:domain/*/_opendistro/_sql",
      "arn:aws:es:*:*:domain/*/_plugin/_sql"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSQuickSightSageMakerPolicy

AWSQuickSightSageMakerPolicy est une [politique AWS gérée](#) qui : fournit un accès aux SageMaker ressources Amazon depuis Amazon QuickSight

Utilisation de cette politique

Vous pouvez vous associer AWSQuickSightSageMakerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 17 janvier 2020, 17:18 UTC
- Heure modifiée : 30 octobre 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModel",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
    "Sid" : "S3objectReadAccess",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : [
      "arn:aws:s3::quicksight-ml.*",
      "arn:aws:s3::sagemaker*"
    ]
  },
  {
    "Sid" : "S3objectUpdateAccess",
    "Effect" : "Allow",
    "Action" : "s3:PutObject",
    "Resource" : "arn:aws:s3::sagemaker*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "S3BucketReadAccess",
    "Effect" : "Allow",
    "Action" : "s3:ListBucket",
    "Resource" : "arn:aws:s3::sagemaker*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSQuickSightTimestreamPolicy

AWSQuickSightTimestreamPolicy est une [politique AWS gérée](#) qui :AWS QuickSight accès aux API AWS Timestream. Les clients peuvent associer cette politique à leur AWS QuickSight rôle pour permettre la récupération des données et des métadonnées.

Utilisation de cette stratégie

Vous pouvez `AWSQuickSightTimestreamPolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 30 septembre 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSReachabilityAnalyzerServiceRolePolicy

AWSReachabilityAnalyzerServiceRolePolicy est une [politique AWS gérée](#) qui : permet à VPC Reachability Analyzer d'accéder aux AWS ressources et de s'intégrer aux AWS organisations en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 23 novembre 2022, 17:12 UTC
- Heure modifiée : 23 juin 2023, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
```

```

    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "tag:GetResources",
    "tiros>CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [

```

```
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSRefactoringToolkitFullAccess

AWSRefactoringToolkitFullAccess est une [politique AWS gérée](#) qui : Cette politique autorise l'utilisation de AWS services avec l'extension AWS Toolkit for .NET Refactoring pour Microsoft Visual Studio. Il est destiné à être rattaché à un AWS profil local. La politique permet de télécharger des artefacts d'application et de télécharger les artefacts qui en résultent depuis Amazon S3. Il permet de créer des applications dans une image de conteneur en utilisant, en stockant AWS CodeBuild et en récupérant les images depuis Amazon Elastic Container Registry (Amazon ECR). Il permet également le déploiement de l'application sur des services de conteneur AWS tels qu'Amazon Elastic Container Service (Amazon ECS), la création facultative de ressources VPC, la connexion facultative à une infrastructure existante telle que Directory AWS Service, et d'autres services connexes.

Utilisation de cette politique

Vous pouvez vous associer AWSRefactoringToolkitFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 octobre 2022, 16:41 UTC
- Heure modifiée : 18 novembre 2023, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "codebuild:CreateProject",
  "codebuild:UpdateProject"
],
"Resource" : "arn:aws:codebuild:*:*:project/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/a2c-generated" : "false"
  }
}
},
{
  "Sid" : "CodeBuildExecutionAccess",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:StartBuild"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/*"
},
{
  "Sid" : "CreateSecurityGroupAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2CreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
```



```
        "aws:RequestTag/a2c-generated" : "false"
    }
}
},
{
  "Sid" : "Ec2CreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "Ec2ModifyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateRouteTable",
    "ec2:AttachInternetGateway",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteTags",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateSubnet",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "Ec2ModifyAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateRouteTable",
      "ec2:AttachInternetGateway",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:DeleteTags",
      "ec2:ModifySubnetAttribute",
      "ec2:ModifyVpcAttribute",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateSubnet",
      "ec2:CreateRoute",
      "ec2:CreateRouteTable"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/application-transformation" : "false"
      }
    }
  },
  {
    "Sid" : "EcrCreateAccess",
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr:TagResource"
    ],
    "Resource" : "arn:*:ecr:*:*:repository/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/a2c-generated" : "false"
      }
    }
  },
  {
    "Sid" : "EcrCreateAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr:TagResource"
    ]
  }
}
```

```
    ],
    "Resource" : "arn:*:ecr:*:*:repository/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/application-transformation" : "false"
      }
    }
  },
  {
    "Sid" : "EcrModifyAccess",
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetLifecyclePolicy",
      "ecr:GetRepositoryPolicy",
      "ecr:ListImages",
      "ecr:ListTagsForResource",
      "ecr:TagResource",
      "ecr:UntagResource"
    ],
    "Resource" : "arn:*:ecr:*:*:repository/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/a2c-generated" : "false"
      }
    }
  },
  {
    "Sid" : "EcrModifyAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetLifecyclePolicy",
      "ecr:GetRepositoryPolicy",
      "ecr:ListImages",
      "ecr:ListTagsForResource",
      "ecr:TagResource",
      "ecr:UntagResource"
    ],
    "Resource" : "arn:*:ecr:*:*:repository/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/application-transformation" : "false"
      }
    }
  }
},
```

```
{
  "Sid" : "EcsCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:CreateService",
    "ecs:RegisterTaskDefinition",
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "EcsCreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:CreateService",
    "ecs:RegisterTaskDefinition",
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcsModifyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateService",
    "ecs:TagResource",
    "ecs:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "EcsModifyAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateService",
    "ecs:TagResource",
    "ecs:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcsReadTaskDefinitionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:DescribeTaskDefinition"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cloudformation.amazonaws.com"
    }
  }
},
{
  "Sid" : "EcsExecuteCommandInSidecar",
  "Effect" : "Allow",
  "Action" : [
    "ecs:ExecuteCommand"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ecs:container-name" : "a2c-sidecar"
    }
  }
},
},
```

```

{
  "Sid" : "EcsExecuteCommandInSidecarATS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:ExecuteCommand"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ecs:container-name" : "application-transformation-sidecar"
    }
  }
},
{
  "Sid" : "CreateEcsServiceLinkedRoleAccess",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "ecs.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudwatchCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:TagResource"
  ],
  "Resource" : [
    "arn:aws:logs::*:log-group:/aws/codebuild/*:*",
    "arn:aws:logs::*:log-group:/aws/ecs/containerinsights/*:*",
    "arn:aws:logs::*:log-group:/aws/ecs/container-logs/*:*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  },
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "a2c-generated"
    ]
  }
}

```

```
    ]
  }
}
},
{
  "Sid" : "CloudwatchCreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:TagResource"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
    "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "application-transformation"
      ]
    }
  }
},
{
  "Sid" : "CloudwatchGetAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
    "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
    "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
},
{
```

```

    "Sid" : "CloudwatchGetAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
      "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/application-transformation" : "false"
      }
    }
  },
  {
    "Sid" : "SsmParameterAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:AddTagsToResource",
      "ssm:GetParameters",
      "ssm:PutParameter",
      "ssm:RemoveTagsFromResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
  },
  {
    "Sid" : "SsmMessagesAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeSessions",
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3ObjectAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteObject",
      "s3:GetObject",

```



```
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::*/refactoringtoolkit*",
    "arn:aws:s3::*/a2c-generated*",
    "arn:aws:s3::*/application-transformation*"
  ]
},
{
  "Sid" : "S3ListAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : [
        "application-transformation",
        "refactoringtoolkit"
      ]
    }
  }
},
{
  "Sid" : "ReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks",
    "clouddirectory:ListDirectories",
    "codebuild:BatchGetProjects",
    "codebuild:BatchGetBuilds",
    "ds:DescribeDirectories",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
```

```

    "ec2:DescribeRegions",
    "ecr:DescribeImages",
    "ecr:DescribeRepositories",
    "ecs:DescribeClusters",
    "ecs:DescribeServices",
    "ecs:DescribeTasks",
    "ecs:ListTagsForResource",
    "ecs:ListTasks",
    "iam:ListRoles",
    "s3:GetBucketLocation",
    "s3:GetBucketVersioning",
    "s3:ListAllMyBuckets",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetECSSLR",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
},
{
  "Sid" : "PortingAssistantFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::aws.portingassistant.dotnet.datastore",
    "arn:aws:s3::aws.portingassistant.dotnet.datastore/*"
  ]
},
{
  "Sid" : "ApplicationTransformationAccess",
  "Effect" : "Allow",
  "Action" : [
    "application-transformation:StartPortingCompatibilityAssessment",
    "application-transformation:GetPortingCompatibilityAssessment",
    "application-transformation:StartPortingRecommendationAssessment",
    "application-transformation:GetPortingRecommendationAssessment",
    "application-transformation:PutLogData",
    "application-transformation:PutMetricData",

```

```

    "application-transformation:StartContainerization",
    "application-transformation:GetContainerization",
    "application-transformation:StartDeployment",
    "application-transformation:GetDeployment"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource" : "arn:aws:kms:*:*:*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "kms:ResourceAliases" : "alias/application-transformation*"
    }
  }
},
{
  "Sid" : "EcrPushAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart",
    "ecr:CompleteLayerUpload",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "ecr:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcrAuthAccess",
  "Effect" : "Allow",

```

```
    "Action" : [
      "ecr:GetAuthorizationToken"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "arn:aws:kms:*:*:*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      },
      "ForAnyValue:StringLike" : {
        "kms:ResourceAliases" : "alias/application-transformation*"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSRefactoringToolkitSidecarPolicy

AWSRefactoringToolkitSidecarPolicy est une [politique AWS gérée](#) qui : Cette politique est destinée à être utilisée par Amazon ECS Tasks créée pour tester des applications à l'aide de l'extension AWS Toolkit for .NET Refactoring pour Microsoft Visual Studio. Cette politique permet de télécharger des artefacts d'application depuis Amazon S3, de communiquer l'état de la tâche à l'aide de AWS Systems Manager et d'autres services requis.

Utilisation de cette stratégie

Vous pouvez les associer `AWSRefactoringToolkitSidecarPolicy` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 octobre 2022, 16:41 UTC
- Heure modifiée : 29 octobre 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3::*/refactoringtoolkit*"
},
{
  "Sid" : "S3ListBucketAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : "refactoringtoolkit*"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSrePostPrivateCloudWatchAccess

AWSrePostPrivateCloudWatchAccess est une [politique AWS gérée](#) qui : fournit un accès privé à Re:POST pour publier des données de métriques CloudWatch

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service

- Heure de création : 15 novembre 2023, 16:37 UTC
- Heure modifiée : 15 novembre 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicy est une [politique AWS gérée](#) qui : Cette politique permet au service Re:Post Space de créer, de gérer et de résoudre les demandes de support créées via l'application Space.

Utilisation de cette politique

Vous pouvez vous associer AWSRepostSpaceSupportOperationsPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 novembre 2023, 21:52 UTC
- Heure modifiée : 26 novembre 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



```
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResilienceHubAssessmentExecutionPolicy

AWSResilienceHubAssessmentExecutionPolicy est une [politique AWS gérée](#) qui : Politique pour le rôle de service AWS Resilience Hub qui permet d'accéder à d'autres AWS services afin d'exécuter une évaluation.

Utilisation de cette politique

Vous pouvez vous associer AWSResilienceHubAssessmentExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 12:32 UTC
- Heure modifiée : 29 octobre 2023, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
```

```
"ec2:DescribeFastSnapshotRestores",
"ec2:DescribeFleets",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribePlacementGroups",
"ec2:DescribeRegions",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ecr:DescribeRegistry",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:ListContainerInstances",
"ecs:ListServices",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
"fis:ListExperiments",
"lambda:GetFunctionConcurrency",
"lambda:GetFunctionConfiguration",
"lambda:ListAliases",
"lambda:ListVersionsByFunction",
"rds:DescribeDBClusterSnapshots",
```

```

    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBInstances",
    "rds:DescribeDBProxies",
    "rds:DescribeDBProxyTargets",
    "rds:DescribeDBSnapshots",
    "rds:DescribeGlobalClusters",
    "resource-groups:GetGroup",
    "resource-groups:ListGroupResources",
    "route53-recovery-control-config:ListClusters",
    "route53-recovery-control-config:ListControlPanels",
    "route53-recovery-control-config:ListRoutingControls",
    "route53-recovery-readiness:GetReadinessCheckStatus",
    "route53-recovery-readiness:GetResourceSet",
    "route53-recovery-readiness:ListReadinessChecks",
    "route53:GetHealthCheck",
    "route53:ListHealthChecks",
    "route53:ListHostedZones",
    "route53:ListResourceRecordSets",
    "s3:GetBucketLocation",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetMultiRegionAccessPointRoutes",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListMultiRegionAccessPoints",
    "servicecatalog:GetApplication",
    "servicecatalog:ListAssociatedResources",
    "sns:GetSubscriptionAttributes",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "ssm:DescribeAutomationExecutions",
    "states:DescribeStateMachine",
    "states:ListStateMachineVersions",
    "states:ListStateMachineAliases",
    "tag:GetResources"
  ],
  "Resource" : "*"
},

```

```
{
  "Sid" : "AWSResilienceHubApiGatewayStatement",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis/*",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/usageplans"
  ]
},
{
  "Sid" : "AWSResilienceHubS3Statement",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
},
{
  "Sid" : "AWSResilienceHubCloudWatchStatement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "ResilienceHub"
    }
  }
},
{
  "Sid" : "AWSResilienceHubSSMStatement",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParametersByPath"
  ],
  "Resource" : "arn:aws:ssm:*::parameter/ResilienceHub/*"
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet auAWS Resource Access Manager

Utilisation de cette stratégie

Vous pouvezAWSResourceAccessManagerFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 4 juin 2019, 17:28 UTC
- Heure modifiée : 4 juin 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule au AWS Resource Access Manager.

Utilisation de cette stratégie

Vous pouvez AWSResourceAccessManagerReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 décembre 2019, 20:58 UTC
- Heure modifiée : 9 décembre 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess est une [politique AWS gérée](#) qui : fournit un accès aux API AWS Resource Access Manager nécessaires à un participant au partage de ressources.

Utilisation de cette stratégie

Vous pouvez les associer `AWSResourceAccessManagerResourceShareParticipantAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 9 décembre 2019, 20:41 UTC
- Heure modifiée : 9 décembre 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSResourceAccessManagerServiceRolePolicy

AWSResourceAccessManagerServiceRolePolicyest une [politiqueAWS gérée qui :](#) [Politique](#) contenant l'accès en lecture seule duAWS Resource Access Manager à la structure des Organizations des clients. Il contient également des autorisations IAM pour supprimer le rôle.

Utilisation politique politique

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 14 novembre 2018, 19:28 UTC
- Heure modifiée : 14 novembre 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégies est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers autorisations gérées](#)

AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations administratives pour accéder aux ressources de l'explorateur de ressources et accorde des autorisations en lecture seule à d'autres AWS services pour prendre en charge cet accès.

Utilisation de cette politique

Vous pouvez vous associer AWSResourceExplorerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 novembre 2022, 20:01 UTC
- Heure modifiée : 14 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",

```

```
    "ram:ListResources",
    "ram:GetResourceShares",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ResourceExplorerSLRAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "resource-explorer-2.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResourceExplorerOrganizationsAccess

AWSResourceExplorerOrganizationsAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations administratives à Resource Explorer et accorde des autorisations en lecture seule à d'autres AWS services pour prendre en charge cet accès. L'administrateur AWS des Organizations a besoin de ces autorisations pour configurer et gérer la recherche multi-comptes dans la console.

Utilisation de cette politique

Vous pouvez vous associer `AWSResourceExplorerOrganizationsAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 novembre 2023, 17:01 UTC
- Heure modifiée : 14 novembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ResourceExplorerGetSLRAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
  },
  {
    "Sid" : "ResourceExplorerCreateSLRAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "resource-explorer-2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "OrganizationsAdministratorAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "resource-explorer-2.amazonaws.com"
        ]
      }
    }
  }
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResourceExplorerReadOnlyAccess

AWSResourceExplorerReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations en lecture seule pour rechercher et afficher les ressources de l'explorateur de ressources et accorde des autorisations en lecture seule à d'autres AWS services pour prendre en charge cet accès.

Utilisation de cette politique

Vous pouvez vous associer AWSResourceExplorerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 novembre 2022, 19:56 UTC
- Heure modifiée : 14 novembre 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicy est une [politique AWS gérée](#) qui : permet à Resource Explorer d'afficher les ressources et les CloudTrail événements en votre nom afin d'indexer vos ressources à des fins de recherche.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 25 octobre 2022, 20:35 UTC
- Heure modifiée : 20 décembre 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/deployments"
  ]
},
{
  "Sid" : "ResourceInventoryAccess",
  "Effect" : "Allow",
  "Action" : [
    "access-analyzer:ListAnalyzers",
    "acm-pca:ListCertificateAuthorities",
    "amplify:ListApps",
    "amplify:ListBackendEnvironments",
    "amplify:ListBranches",
    "amplify:ListDomainAssociations",
    "amplifyuibuilder:ListComponents",
    "amplifyuibuilder:ListThemes",
    "app-integrations:ListEventIntegrations",
    "apprunner:ListServices",
    "apprunner:ListVpcConnectors",
    "appstream:DescribeAppBlocks",
    "appstream:DescribeApplications",
    "appstream:DescribeFleets",
    "appstream:DescribeImageBuilders",
    "appstream:DescribeStacks",
    "appsync:ListGraphQLApis",
    "aps:ListRuleGroupsNamespaces",
    "aps:ListWorkspaces",
    "athena:ListDataCatalogs",
    "athena:ListWorkGroups",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListReportPlans",
    "batch:DescribeComputeEnvironments",
    "batch:DescribeJobQueues",
    "batch:ListSchedulingPolicies",
    "cloudformation:ListStacks",
    "cloudformation:ListStackSets",
    "cloudfront:ListCachePolicies",
    "cloudfront:ListCloudFrontOriginAccessIdentities",
    "cloudfront:ListDistributions",
    "cloudfront:ListFieldLevelEncryptionConfigs",
```

```
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListOriginRequestPolicies",
"cloudfront:ListRealtimeLogConfigs",
"cloudfront:ListResponseHeadersPolicies",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"codeartifact:ListDomains",
"codeartifact:ListRepositories",
"codebuild:ListProjects",
"codecommit:ListRepositories",
"codeguru-profiler:ListProfilingGroups",
"codepipeline:ListPipelines",
"codestar-connections:ListConnections",
"cognito-identity:ListIdentityPools",
"cognito-idp:ListUserPools",
"databrew:ListDatasets",
"databrew:ListRecipes",
"databrew:ListRulesets",
"detective:ListGraphs",
"ds:DescribeDirectories",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeCapacityReservationFleets",
"ec2:DescribeCapacityReservations",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeElasticGpus",
"ec2:DescribeExportImageTasks",
"ec2:DescribeExportTasks",
"ec2:DescribeFleets",
"ec2:DescribeFlowLogs",
"ec2:DescribeFpgaImages",
"ec2:DescribeHostReservations",
"ec2:DescribeHosts",
"ec2:DescribeImages",
```

```
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstanceEventWindows",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeIpamPools",
"ec2:DescribeIpams",
"ec2:DescribeIpamScopes",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInsightsAccessScopeAnalyses",
"ec2:DescribeNetworkInsightsAccessScopes",
"ec2:DescribeNetworkInsightsAnalyses",
"ec2:DescribeNetworkInsightsPaths",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeReservedInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeSubnets",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPolicyTables",
"ec2:DescribeTransitGatewayRouteTableAnnouncements",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeVerifiedAccessEndpoints",
"ec2:DescribeVerifiedAccessGroups",
"ec2:DescribeVerifiedAccessInstances",
"ec2:DescribeVerifiedAccessTrustProviders",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
```

```
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetSubnetCidrReservations",
"ecr:DescribeRepositories",
"ecr-public:DescribeRepositories",
"ecs:DescribeCapacityProviders",
"ecs:DescribeServices",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:ListServices",
"ecs:ListTaskDefinitions",
"ecs:ListTasks",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeReservedCacheNodes",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"emr-serverless:ListApplications",
"es:ListDomainNames",
"events:ListEventBuses",
"events:ListRules",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"finspace:ListEnvironments",
"firehose:ListDeliveryStreams",
```

```
"fis:ListExperimentTemplates",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"frauddetector:GetEntityTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetLabels",
"frauddetector:GetOutcomes",
"frauddetector:GetVariables",
"gamelift:ListAliases",
"geo:ListPlaceIndexes",
"geo:ListTrackers",
"greengrass:ListComponents",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"glue:GetDatabases",
"glue:GetJobs",
"glue:GetTables",
"glue:GetTriggers",
"greengrass:ListComponentVersions",
"greengrass:ListGroups",
"healthlake:ListFHIRDatastores",
"iam:ListGroups",
"iam:ListInstanceProfiles",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
```

```
"iotanalytics:ListPipelines",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iot:ListJobTemplates",
"iot:ListAuthorizers",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListSecurityProfiles",
"iot:ListThings",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListGateways",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListWorkspaces",
"kafka:ListConfigurations",
"kms:ListKeys",
"ivs:ListChannels",
"ivs:ListStreamKeys",
"kafka:ListClusters",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisvideo:ListStreams",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lex:ListBots",
"lex:ListBotAliases",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"lookoutmetrics:ListAlerts",
"lookoutvision:ListProjects",
"mediapackage:ListChannels",
```



```
"mediapackage:ListOriginEndpoints",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mq:ListBrokers",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeACLs",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeUsers",
"mobiletargeting:GetApps",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTemplates",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetDevices",
"networkmanager:GetLinks",
"networkmanager:ListAttachments",
"networkmanager:ListCoreNetworks",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:ListAccounts",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListDelegatedAdministrators",
"panorama:ListPackages",
"personalize:ListDatasetGroups",
"personalize:ListDatasets",
"personalize:ListSchemas",
"qlldb:ListJournalKinesisStreamsForLedger",
"qlldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
```

```
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeReservedDBInstances",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"rekognition:DescribeProjects",
"resiliencehub:ListApps",
"resiliencehub:ListResiliencyPolicies",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListViews",
"resource-groups:ListGroups",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverRules",
"s3:GetBucketLocation",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListStorageLensConfigurations",
"sagemaker:ListModels",
"sagemaker:ListNotebookInstances",
"secretsmanager:ListSecrets",
"servicecatalog:ListApplications",
"servicecatalog:ListAttributeGroups",
"signer:ListSigningProfiles",
"sns:ListTopics",
"sqs:ListQueues",
```

```
    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeMaintenanceWindows",
    "ssm:DescribeMaintenanceWindowTargets",
    "ssm:DescribeMaintenanceWindowTasks",
    "ssm:DescribeParameters",
    "ssm:DescribePatchBaselines",
    "ssm-incidents:ListResponsePlans",
    "ssm:ListAssociations",
    "ssm:ListDocuments",
    "ssm:ListInventoryEntries",
    "ssm:ListResourceDataSync",
    "states:ListActivities",
    "states:ListStateMachines",
    "timestream:ListDatabases",
    "wisdom:listAssistantAssociations",
    "wisdom:ListAssistants",
    "wisdom:listKnowledgeBases"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSResourceGroupsReadOnlyAccess

AWSResourceGroupsReadOnlyAccess est une [politique AWS gérée](#) qui : Il s'agit de la politique en lecture seule pour les AWS Resource Groups

Utilisation de cette stratégie

Vous pouvez AWSResourceGroupsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 7 mars 2018, 10:27 UTC
- Heure modifiée : 5 février 2019, 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
```

```
    "glacier:DescribeVault",
    "glacier:ListTagsForVault",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:ListTagsForStream",
    "opsworks:DescribeStacks",
    "opsworks:ListTags",
    "rds:DescribeDBInstances",
    "rds:DescribeDBSnapshots",
    "rds:ListTagsForResource",
    "redshift:DescribeClusters",
    "redshift:DescribeTags",
    "route53domains:ListDomains",
    "route53:ListHealthChecks",
    "route53:GetHealthCheck",
    "route53:ListHostedZones",
    "route53:GetHostedZone",
    "route53:ListTagsForResource",
    "storagegateway:ListGateways",
    "storagegateway:DescribeGatewayInformation",
    "storagegateway:ListTagsForResource",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "ssm:ListDocuments"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess` est une [politique AWS gérée](#) qui : fournit un accès complet à AWS RoboMaker via le SDK AWS Management Console et. fournit également un accès sélectif aux services connexes (par exemple, S3, IAM).

Utilisation de la politique

Vous pouvez `AWSRoboMaker_FullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails de politique

- Type : politique AWS gérée
- Heure de création : 10 septembre 2020, 18:34 UTC
- Heure modifiée : 16 septembre 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ecr:BatchGetImage",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ecr-public:DescribeImages",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "robomaker.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSRoboMakerReadOnlyAccess

AWSRoboMakerReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule AWS RoboMaker via le SDK AWS Management Console et

Utilisation de cette stratégie

Vous pouvez AWSRoboMakerReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 novembre 2018, 05:30 UTC
- Heure modifiée : 28 août 2020, 23h10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
```



```
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSRoboMakerServicePolicy

AWSRoboMakerServicePolicy est une [politique AWS gérée](#) qui : politique RoboMaker de service

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 26 novembre 2018, 06:30 UTC
- Heure modifiée : 11 novembre 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations de la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    }
  ]
}
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AWSRoboMakerServiceRolePolicy

AWSRoboMakerServiceRolePolicy est une [politique AWS gérée](#) qui : politique RoboMaker de service

Utilisation de cette stratégie

Vous pouvez `AWSRoboMakerServiceRolePolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 novembre 2018, 05:33 UTC
- Heure modifiée : 26 novembre 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
```

```
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetFunctionDefinitionVersion",
    "greengrass:GetAssociatedRole",
    "lambda:CreateFunction"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "lambda:UpdateFunctionCode",
    "lambda:GetFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSRolesAnywhereServicePolicy

AWSRolesAnywhereServicePolicy est une [politique AWS gérée](#) qui : autorise IAM Roles Anywhere à publier des mesures de service/d'utilisation CloudWatch et à vérifier le statut des autorités de certification privées en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette stratégie à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 5 juillet 2022, 15:26 UTC
- Heure modifiée : 5 juillet 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/RolesAnywhere",
          "AWS/Usage"
        ]
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy est une [politique AWS gérée](#) qui : autorise le service Amazon S3 on Outposts à gérer les ressources du réseau EC2 en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 03 octobre 2023, 20:32 UTC
- Heure modifiée : 3 octobre 2023, 20:32 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS30nOutpostsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "S3 On Outposts"
    }
  },
  "Sid" : "CreateTagsForCreateNetworkInterface"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:ipv4pool-ec2/*"
  ],
  "Sid" : "AllocateIpAddress"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:elastic-ip/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "S3 On Outposts"
    }
  },
  "Sid" : "CreateTagsForAllocateIpAddress"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute",
```

```
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:AssociateAddress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
    }
  },
  "Sid" : "ReleaseVpcResources"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateNetworkInterface",
        "AllocateAddress"
      ],
      "aws:RequestTag/CreatedBy" : [
        "S3 On Outposts"
      ]
    }
  },
  "Sid" : "CreateTags"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSavingsPlansFullAccess

AWSSavingsPlansFullAccess est une [police AWS gérée](#) qui : Fournit un accès complet au service des Savings Plans

Utilisation de cette stratégie

Vous pouvez AWSSavingsPlansFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 novembre 2019, 22:45 UTC
- Heure modifiée : 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule au service des Savings Plans

Utilisation de cette stratégie

Vous pouvez AWSSavingsPlansReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 novembre 2019, 22:45 UTC
- Heure modifiée : 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "savingsplans:Describe*",
    "savingsplans:List*"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS SecurityHubFullAccess

AWS SecurityHubFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet pour utiliser AWS Security Hub.

Utilisation de cette politique

Vous pouvez vous associer AWS SecurityHubFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 23:54 UTC
- Heure modifiée : 16 novembre 2023, 21h10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSecurityHubOrganizationsAccess

AWSecurityHubOrganizationsAccess est une [politique AWS gérée](#) qui : accorde l'autorisation d'activer et de gérer AWS Security Hub au sein d'une organisation. Cela inclut l'activation du service dans l'ensemble de l'organisation et la détermination du compte d'administrateur délégué pour le service.

Utilisation de cette politique

Vous pouvez vous associer AWSecurityHubOrganizationsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 mars 2021, 20:53 UTC
- Heure modifiée : 16 novembre 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Sid" : "OrganizationPermissions",
"Effect" : "Allow",
"Action" : [
  "organizations:ListAccounts",
  "organizations:DescribeOrganization",
  "organizations:ListRoots",
  "organizations:ListDelegatedAdministrators",
  "organizations:ListAWSServiceAccessForOrganization",
  "organizations:ListOrganizationalUnitsForParent",
  "organizations:ListAccountsForParent",
  "organizations:DescribeAccount",
  "organizations:DescribeOrganizationalUnit"
],
"Resource" : "*"
},
{
  "Sid" : "OrganizationPermissionsEnable",
  "Effect" : "Allow",
  "Action" : "organizations:EnableAWSServiceAccess",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
    }
  }
},
{
  "Sid" : "OrganizationPermissionsDelegatedAdmin",
  "Effect" : "Allow",
  "Action" : [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "arn:aws:organizations::*:account/o-*/*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
    }
  }
}
]
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSecurityHubReadOnlyAccess

AWSSecurityHubReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux ressources du AWS Security Hub

Utilisation de cette politique

Vous pouvez vous associer AWSSecurityHubReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 01:34 UTC
- Heure modifiée : 22 février 2024, 23h45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "AWSSecurityHubReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "securityhub:Get*",
    "securityhub:List*",
    "securityhub:BatchGet*",
    "securityhub:Describe*"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy est une [politique AWS gérée](#) qui : un rôle lié à un service est requis pour que AWS Security Hub puisse accéder à vos ressources.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 27 novembre 2018, 23:47 UTC
- Heure modifiée : 27 novembre 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
```

```

    "securityhub:BatchGetSecurityControls",
    "securityhub:BatchGetStandardsControlAssociations",
    "securityhub:CreateMembers",
    "securityhub>DeleteMembers",
    "securityhub:DescribeHub",
    "securityhub:DescribeOrganizationConfiguration",
    "securityhub:DescribeStandards",
    "securityhub:DescribeStandardsControls",
    "securityhub:DisassociateFromAdministratorAccount",
    "securityhub:DisassociateMembers",
    "securityhub:DisableSecurityHub",
    "securityhub:EnableSecurityHub",
    "securityhub:GetEnabledStandards",
    "securityhub>ListStandardsControlAssociations",
    "securityhub>ListSecurityControlDefinitions",
    "securityhub:UpdateOrganizationConfiguration",
    "securityhub:UpdateSecurityControl",
    "securityhub:UpdateSecurityHubConfiguration",
    "securityhub:UpdateStandardsControl"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecurityHubServiceRoleConfigPermissions",
  "Effect" : "Allow",
  "Action" : [
    "config:PutConfigRule",
    "config>DeleteConfigRule",
    "config:GetComplianceDetailsByConfigRule"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
},
{
  "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "securityhub.amazonaws.com"
      ]
    }
  ]
}

```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceCatalogAdminFullAccess

AWSServiceCatalogAdminFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet aux fonctionnalités d'administration du catalogue de services

Utilisation de cette stratégie

Vous pouvez AWSServiceCatalogAdminFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 février 2018, 17:19 UTC
- Heure modifiée : 13 avril 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "cloudformation:CreateUploadBucket",
  "cloudformation:GetTemplateSummary",
  "cloudformation:ValidateTemplate",
  "iam:GetGroup",
  "iam:GetRole",
  "iam:GetUser",
  "iam:ListGroups",
  "iam:ListRoles",
  "iam:ListUsers",
  "servicecatalog:Get*",
  "servicecatalog:Scan*",
  "servicecatalog:Search*",
  "servicecatalog:List*",
  "servicecatalog:TagResource",
  "servicecatalog:UntagResource",
  "servicecatalog:SyncResource",
  "ssm:DescribeDocument",
  "ssm:GetAutomationExecution",
  "ssm:ListDocuments",
  "ssm:ListDocumentVersions",
  "config:DescribeConfigurationRecorders",
  "config:DescribeConfigurationRecorderStatus"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:Accept*",
    "servicecatalog:Associate*",
    "servicecatalog:Batch*",
    "servicecatalog:Copy*",
    "servicecatalog:Create*",
    "servicecatalog>Delete*",
    "servicecatalog:Describe*",
    "servicecatalog:Disable*",
    "servicecatalog:Disassociate*",
    "servicecatalog:Enable*",
    "servicecatalog:Execute*",
    "servicecatalog:Import*",
    "servicecatalog:Provision*",
    "servicecatalog:Put*",
    "servicecatalog:Reject*",
```

```

    "servicecatalog:Terminate*",
    "servicecatalog:Update*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "servicecatalog.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceCatalogAdminReadOnlyAccess

AWSServiceCatalogAdminReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux fonctionnalités d'administration du Service Catalog

Utilisation de cette stratégie

Vous pouvez `AWSServiceCatalogAdminReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 octobre 2019, 18:53 UTC
- Heure modifiée : 25 octobre 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/SC-*",
      "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
      "arn:aws:cloudformation:*:*:changeSet/SC-*",
      "arn:aws:cloudformation:*:*:stackset/SC-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:GetTemplateSummary",
      "iam:GetGroup",
      "iam:GetRole",
      "iam:GetUser",
      "iam:ListGroups",
      "iam:ListRoles",
      "iam:ListUsers",
      "servicecatalog:Get*",
      "servicecatalog:List*",
      "servicecatalog:Describe*",
      "servicecatalog:ScanProvisionedProducts",
      "servicecatalog:Search*",
      "ssm:DescribeDocument",
      "ssm:GetAutomationExecution",
      "ssm:ListDocuments",
      "ssm:ListDocumentVersions",
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux fonctionnalités de Service Catalog App Registry

Utilisation de cette politique

Vous pouvez vous associer AWSServiceCatalogAppRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 novembre 2020, 22:25 UTC
- Heure modifiée : 7 décembre 2023, 21h50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```

        "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
    }
}
},
{
    "Sid" : "AppRegistryResourceGroupsIntegration",
    "Effect" : "Allow",
    "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups>DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
    }
},
{
    "Sid" : "AppRegistryServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/servicecatalog-appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
    }
},
{
    "Sid" : "AppRegistryOperations",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",

```

```

    "servicecatalog:UpdateApplication",
    "servicecatalog>DeleteApplication",
    "servicecatalog:ListApplications",
    "servicecatalog:AssociateResource",
    "servicecatalog:DisassociateResource",
    "servicecatalog:GetAssociatedResource",
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup",
    "servicecatalog:ListAssociatedAttributeGroups",
    "servicecatalog>CreateAttributeGroup",
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog>DeleteAttributeGroup",
    "servicecatalog:GetAttributeGroup",
    "servicecatalog:ListAttributeGroups",
    "servicecatalog:SyncResource",
    "servicecatalog:ListAttributeGroupsForApplication",
    "servicecatalog:GetConfiguration",
    "servicecatalog:PutConfiguration"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AppRegistryResourceTagging",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:ListTagsForResource",
    "servicecatalog:UntagResource",
    "servicecatalog:TagResource"
  ],
  "Resource" : "arn:aws:servicecatalog:*:*:*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

AWSServiceCatalogAppRegistryReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux fonctionnalités du registre des applications de Service Catalog

Utilisation de cette stratégie

Vous pouvez les associer AWSServiceCatalogAppRegistryReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 12 novembre 2020, 22:34 UTC
- Heure modifiée : 17 novembre 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",

```

```
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS ServiceCatalogAppRegistryServiceRolePolicy

AWS ServiceCatalogAppRegistryServiceRolePolicy est une [politique AWS gérée](#) qui :
Permet à Service Catalog AppRegistry de gérer des Resource Groups en votre nom

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 18 mai 2021, 22h18 UTC
- Heure modifiée : 26 octobre 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups>DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:GetGroup",
    "resource-groups:GetGroupConfiguration"
  ],
  "Resource" : [
    "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
    "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet aux fonctionnalités du catalogue de services pour les utilisateurs finaux

Utilisation de cette stratégie

Vous pouvez les associer AWSServiceCatalogEndUserFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 février 2018, 17:22 UTC
- Heure modifiée : 10 juillet 2019, 20h30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation>DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
    },
  ],
}
```

```
"Resource" : [
  "arn:aws:cloudformation:*:*:stack/SC-*",
  "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
  "arn:aws:cloudformation:*:*:changeSet/SC-*",
  "arn:aws:cloudformation:*:*:stackset/SC-*"
],
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog>CreateProvisionedProductPlan",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ExecuteProvisionedProductPlan",
    "servicecatalog>DeleteProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteProvisionedProductServiceAction",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
}
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "servicecatalog:userLevel" : "self"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceCatalogEndUserReadOnlyAccess

AWSServiceCatalogEndUserReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux fonctionnalités des utilisateurs finaux de Service Catalog

Utilisation de cette stratégie

Vous pouvez AWSServiceCatalogEndUserReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 octobre 2019, 18:49 UTC
- Heure modifiée : 25 octobre 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",

```

```

    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWS ServiceCatalogOrgsDataSyncServiceRolePolicy

AWS ServiceCatalogOrgsDataSyncServiceRolePolicy est une [politique AWS gérée](#) qui :
 Une politique de rôle liée aux services pour AWS ServiceCatalog se synchroniser avec la structure organisationnelle de l'AWS Organizations


```
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les les les les lesAWS les les les les les les les les les les les les les les les](#)

AWSServiceCatalogSyncServiceRolePolicy

AWSServiceCatalogSyncServiceRolePolicy est une [politique AWS gérée](#) qui : Un rôle lié à un service permettant de AWS ServiceCatalog synchroniser les artefacts de provisionnement à partir de référentiels sources

Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 15 novembre 2022, 21:20 UTC
- Heure modifiée : 15 novembre 2022, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La stratégie est la version qui définit les autorisations Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog>DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog>CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AWSServiceRoleForAmazonEKSNodegroup

AWSServiceRoleForAmazonEKSNodegroup est une [politique AWS gérée](#) qui : Autorisations requises pour gérer les groupes de nœuds dans le compte du client. Ces politiques concernent la gestion des ressources suivantes : AutoscalingGroups, SecurityGroups, LaunchTemplates et InstanceProfiles.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 07 novembre 2019, 01:34 UTC
- Heure modifiée : 4 janvier 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
```

```

    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DescribeInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks" : "*"
    }
  }
},
{
  "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DescribeInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks:nodegroup-name" : "*"
    }
  }
},
{
  "Sid" : "LaunchTemplateRelatedPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteLaunchTemplate",
    "ec2>CreateLaunchTemplateVersion"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/eks:nodegroup-name" : "*"
    }
  }
},

```

```
{
  "Sid" : "AutoscalingRelatedPermissions",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:CompleteLifecycleAction",
    "autoscaling:PutLifecycleHook",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:EnableMetricsCollection"
  ],
  "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
},
{
  "Sid" : "AllowAutoscalingToCreateSLR",
  "Effect" : "Allow",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "autoscaling.amazonaws.com"
    }
  },
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*"
},
{
  "Sid" : "AllowASGCreationByEKS",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:CreateAutoScalingGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "eks",
        "eks:cluster-name",
        "eks:nodegroup-name"
      ]
    }
  }
},
{
```

```
"Sid" : "AllowPassRoleToAutoscaling",
"Effect" : "Allow",
"Action" : "iam:PassRole",
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "autoscaling.amazonaws.com"
  }
},
{
  "Sid" : "AllowPassRoleToEC2",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "PermissionsToManageResourcesForNodegroups",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "ec2:CreateLaunchTemplate",
    "ec2:DescribeInstances",
    "iam:GetInstanceProfile",
    "ec2:DescribeLaunchTemplates",
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:CreateSecurityGroup",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:RunInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:GetConsoleOutput",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "PermissionsToCreateAndManageInstanceProfiles",
"Effect" : "Allow",
"Action" : [
  "iam:CreateInstanceProfile",
  "iam>DeleteInstanceProfile",
  "iam:RemoveRoleFromInstanceProfile",
  "iam:AddRoleToInstanceProfile"
],
"Resource" : "arn:aws:iam::*:instance-profile/eks-*"
},
{
  "Sid" : "PermissionsToManageEKSandKubernetesTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "eks",
        "eks:cluster-name",
        "eks:nodegroup-name",
        "kubernetes.io/cluster/*"
      ]
    }
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY est une [politique AWS gérée](#) qui : Fournit un accès aux ressources de Systems Manager utilisées par les CloudWatch alarmes

Utilisation cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 1 octobre 2020, 09:49 UTC
- Heure modifiée : 01 octobre 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie par défaut. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow"
  }
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy est un [AWS politique gérée](#) qui : Permet CloudWatch pour accéder aux métriques RDS Performance Insights en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type: Politique relative aux rôles liés aux services
- Heure de création: 07 septembre 2023, 09h32 UTC
- Heure modifiée :07 septembre 2023, 09h32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

AWSServiceRoleForCodeGuru-Profiler

AWSServiceRoleForCodeGuru-Profiler est une [politique AWS gérée](#) qui : Un rôle lié à un service est requis pour qu'Amazon CodeGuru Profiler envoie des notifications en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 26 juin 2020, 22:04 UTC

- Heure modifiée : 26 juin 2020, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRoleForCodeWhispererPolicy

AWSServiceRoleForCodeWhispererPolicyest une [politique AWS gérée](#) qui : Ce rôle accorde les autorisations d'accès CodeWhisperer aux données de votre compte pour calculer la facturation,

permet de créer et d'accéder à des rapports de sécurité sur Amazon CodeGuru, et d'émettre des données vers CloudWatch.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 24 mars 2023, 19:39 UTC
- Heure modifiée : 1 mars 2024, 23h35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  {
```

```
"Sid" : "sid2",
"Effect" : "Allow",
"Action" : [
  "sso:ListProfileAssociations",
  "sso:ListProfiles",
  "sso:ListDirectoryAssociations",
  "sso:DescribeRegisteredRegions",
  "sso:GetProfile",
  "sso:GetManagedApplicationInstance",
  "sso:ListApplicationAssignments",
  "sso:DescribeInstance"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "sid3",
  "Effect" : "Allow",
  "Action" : [
    "codeguru-security:CreateUploadUrl"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "sid4",
  "Effect" : "Allow",
  "Action" : [
    "codeguru-security:CreateScan",
    "codeguru-security:GetScan",
    "codeguru-security:ListFindings",
    "codeguru-security:GetFindings"
  ],
  "Resource" : [
    "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
  ]
},
{
  "Sid" : "sid5",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/CodeWhisperer"
        ]
      }
    }
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForEC2ScheduledInstances

AWSServiceRoleForEC2ScheduledInstances est une [politique AWS gérée](#) qui : Permet aux instances planifiées EC2 de lancer et de gérer des instances ponctuelles.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 octobre 2017, 18:31 UTC
- Heure modifiée : 12 octobre 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy est une [politiqueAWS gérée](#) qui :AWS GroundStation utilise ce rôle lié à un service pour appeler EC2 afin de rechercher des adresses IPv4 publiques

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 13 décembre 2022, 23:52 UTC
- Heure modifiée : 13 décembre 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec politiques](#)

AWSServiceRoleForImageBuilder

AWSServiceRoleForImageBuilder est une [politique AWS gérée](#) qui : autorise EC2 ImageBuilder à appeler AWS des services en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 29 novembre 2019, 22:02 UTC
- Heure modifiée : 19 octobre 2023, 21h30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Version de la politique

Version de la politique : v19 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn",
        "vmie.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:StartInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:CreateImage",
    "ec2:CreateLaunchTemplate",
    "ec2:DeregisterImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2: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-*"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForIoTSiteWise

AWSServiceRoleForIoTSiteWise est une [politique AWS gérée](#) qui : permet SiteWise à AWS l'IoT de fournir et de gérer des passerelles ainsi que d'interroger des données. La politique inclut les autorisations AWS Greengrass requises pour le déploiement dans des groupes, les autorisations

AWS Lambda pour créer et mettre à jour des fonctions préfixées par des services, et les autorisations IoT AWS Analytics pour interroger les données des banques de données.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 14 novembre 2018, 19:19 UTC
- Heure modifiée : 13 novembre 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    }
  ]
}
```

```

    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITWISE"
          ]
        }
      }
    }
  ]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy est une [politique AWS gérée](#) qui : Permet au service Log Delivery de fournir des journaux en appelant la destination du journal en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 octobre 2019, 17:31 UTC
- Heure modifiée : 15 juillet 2021, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ]
    }
  ],
}
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/LogDeliveryEnabled" : "true"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRoleForMonitronPolicy

AWSServiceRoleForMonitronPolicy est une [politiqueAWS gérée](#) qui : accorde à Amazon Monitron les autorisations nécessaires pour gérer lesAWS ressources, y compris l'attribution d'utilisateursAWS SSO en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 2 décembre 2020, 19:06 UTC
- Heure modifiée : 29 septembre 2022, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées](#)

AWSServiceRoleForNeptuneGraphPolicy

AWSServiceRoleForNeptuneGraphPolicyest une [politique AWS gérée](#) qui : fournit un accès à Cloudwatch pour publier des statistiques et des journaux opérationnels et d'utilisation pour Amazon Neptune

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 29 novembre 2023, 14:03 UTC
- Heure modifiée : 29 novembre 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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



```
    ]
  }
}
},
{
  "Sid" : "GraphLogGroup",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/neptune/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "GraphLogEvents",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

AWSServiceRoleForPrivateMarketplaceAdminPolicy est une [politique AWS gérée](#) qui : fournit des autorisations pour décrire et mettre à jour les ressources de Private Marketplace et pour décrire AWS les Organizations

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 14 février 2024, 22:28 UTC
- Heure modifiée : 14 février 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
```

```

    "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
    "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
    "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
    "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
  ]
},
{
  "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:DescribeChangeSet"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PrivateMarketplaceCatalogListPermissions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:ListEntities",
    "aws-marketplace:ListChangeSets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:StartChangeSet"
  ],
  "Condition" : {
    "StringEquals" : {
      "catalog:ChangeType" : [
        "AssociateAudience",
        "DisassociateAudience"
      ]
    }
  },
  "Resource" : [
    "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
    "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
  ]
},
{
  "Sid" : "PrivateMarketplaceOrganizationPermissions",

```

```
"Effect" : "Allow",
"Action" : [
  "organizations:DescribeAccount",
  "organizations:DescribeOrganizationalUnit",
  "organizations:ListDelegatedAdministrators",
  "organizations:ListChildren"
],
"Resource" : [
  "*"
]
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSServiceRoleForSMS

AWSServiceRoleForSMS est une [politique AWS gérée](#) qui : fournit un accès aux AWS services et aux ressources nécessaires à la migration des instances de service, AWS notamment vers EC2, S3 et Cloudformation.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 6 août 2019, 18:39 UTC
- Heure modifiée : 15 octobre 2020, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

Version de la politique

Version de la politique :v10 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation>DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
```

```
    "cloudformation:DescribeStackResources",
    "cloudformation:GetTemplate"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
```

```
"Effect" : "Allow",
"Action" : "ssm:SendCommand",
"Resource" : [
  "arn:aws:ssm:*::document/AWS-RunRemoteScript",
  "arn:aws:s3:::sms-app-*"
],
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/SMSJobId" : [
```

```
        "sms-*"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopyImage",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSnapshotAttribute",
      "ec2:DeregisterImage",
      "ec2:ImportImage",
      "ec2:DescribeImportImageTasks",
      "ec2:GetEbsEncryptionByDefault"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:GetInstanceProfile"
    ],
    "Resource" : "*"
  },
  {
```



```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "cloudformation.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "*"
  },
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyInstanceAttribute",
    "ec2:StopInstances",
    "ec2:StartInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "applicationinsights:Describe*",
    "applicationinsights:List*",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "applicationinsights:CreateApplication",
    "applicationinsights:CreateComponent",
    "applicationinsights:UpdateApplication",
    "applicationinsights>DeleteApplication",
    "applicationinsights:UpdateComponentConfiguration",
    "applicationinsights>DeleteComponent"
  ],
}
```

```

    "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:GetGroup",
      "resource-groups:UpdateGroup",
      "resource-groups>DeleteGroup"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "application-insights.amazonaws.com"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRolePolicyForBackupReports

AWSServiceRolePolicyForBackupReport est une [politique AWS gérée](#) qui : fournit des autorisations AWS Backup pour créer des rapports de conformité en votre nom

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 août 2021, 21:16 UTC
- Heure modifiée : 10 mars 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ]
    }
  ],
}
```

```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config:BatchGetResourceConfig",
      "config:SelectResourceConfig",
      "config:DescribeConfigurationAggregators",
      "config:SelectAggregateResourceConfig",
      "config:DescribeConfigRuleEvaluationStatus",
      "config:DescribeConfigRules",
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:GetComplianceDetailsByConfigRule",
      "config:PutConfigRule",
      "config>DeleteConfigRule"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config>DeleteConfigurationAggregator",
      "config:PutConfigurationAggregator"
    ],
    "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
  }
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting est une [politique AWS gérée](#) qui :

Cette politique contient des autorisations permettant de tester les restaurations et de nettoyer les ressources créées lors des tests.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 10 novembre 2023, 23:37 UTC
- Heure modifiée : 14 février 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
```

```

    "backup:GetRecoveryPointRestoreMetadata",
    "backup:ListBackupVaults",
    "backup:ListProtectedResources",
    "backup:ListProtectedResourcesByBackupVault",
    "backup:ListRecoveryPointsByBackupVault",
    "backup:ListRecoveryPointsByResource",
    "backup:ListTags",
    "backup:StartRestoreJob"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IamPassRole",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "backup.amazonaws.com"
    }
  }
},
{
  "Sid" : "DescribeActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeTags",
    "ec2:DescribeVolumes",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "fsx:ListTagsForResource",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups",
    "rds:ListTagsForResource",
    "redshift:DescribeClusters"
  ],
  "Resource" : "*"
},

```

```
{
  "Sid" : "DeleteActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVolume",
    "ec2:TerminateInstances",
    "elasticfilesystem:DeleteFilesystem",
    "elasticfilesystem:DeleteMountTarget",
    "rds:DeleteDBCluster",
    "rds:DeleteDBInstance",
    "fsx:DeleteFileSystem",
    "fsx:DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/awsbackup-restore-test" : "false"
    }
  }
},
{
  "Sid" : "DdbDeleteActions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DeleteTable",
    "dynamodb:DescribeTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RedshiftDeleteActions",
  "Effect" : "Allow",
  "Action" : "redshift:DeleteCluster",
  "Resource" : "arn:aws:redshift:*:*:cluster/awsbackup-restore-test-*"
},
{
  "Sid" : "S3DeleteActions",
  "Effect" : "Allow",
  "Action" : [
```



```
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "TimestreamDeleteActions",
  "Effect" : "Allow",
  "Action" : "timestream:DeleteTable",
  "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy est une [politique AWS gérée](#) qui : fournit à l'équipe d'intervention AWS DDoS un accès limité à vous pour vous aider. Compte AWS à atténuer les attaques DDoS lors d'un événement de haute gravité.

Utilisation de cette stratégie

Vous pouvez les associer AWSShieldDRTAccessPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 5 juin 2018, 22:29 UTC

- Heure modifiée : 15 décembre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*"
      ]
    }
  ]
}
```

```
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSShieldServiceRolePolicy

AWSShieldServiceRolePolicy est une [politique AWS gérée](#) qui : Permet à AWS Shield d'accéder aux AWS ressources en votre nom afin de fournir une protection contre les attaques DDoS.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 novembre 2021, 19:17 UTC
- Heure modifiée : 17 novembre 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSMForSAPServiceLinkedRolePolicy

AWSSSMForSAPServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : fournit à AWS Systems Manager for SAP les autorisations nécessaires pour gérer et intégrer les logiciels SAPAWS.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 16 novembre 2022, 01:18 UTC
- Heure modifiée : 21 novembre 2023, 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
```

```

    "Action" : [
      "events:DeleteRule",
      "events:PutTargets",
      "events:DescribeRule",
      "events:PutRule",
      "events:RemoveTargets"
    ],
    "Resource" : [
      "arn:*:events:*:*:rule/SSMSAPManagedRule*",
      "arn:*:events:*:*:event-bus/default"
    ]
  },
  {
    "Sid" : "DocumentActions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
      "arn:*:ssm:*:*:document/AWSSSMSAP*",
      "arn:*:ssm:*:*:document/AWSSAP*"
    ]
  },
  {
    "Sid" : "CustomerSendCommand",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:*:ec2:*:*:instance/*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "ssm:resourceTag/SSMForSAPManaged" : "True"
      }
    }
  },
  {
    "Sid" : "InstanceTagActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "arn:*:ec2:*:*:instance/*",

```

```

"Condition" : {
  "Null" : {
    "aws:RequestTag/awsApplication" : "false"
  },
  "StringEqualsIgnoreCase" : {
    "ec2:ResourceTag/SSMForSAPManaged" : "True"
  }
},
{
  "Sid" : "DescribeTag",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeTags",
  "Resource" : "*"
},
{
  "Sid" : "GetApplication",
  "Effect" : "Allow",
  "Action" : "servicecatalog:GetApplication",
  "Resource" : "arn:*:servicecatalog:*:*:*"
},
{
  "Sid" : "UpdateOrDeleteApplication",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DeleteApplication",
    "servicecatalog:UpdateApplication"
  ],
  "Resource" : "arn:*:servicecatalog:*:*:*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "CreateApplication",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:TagResource",
    "servicecatalog:CreateApplication"
  ],
  "Resource" : "arn:*:servicecatalog:*:*:*",
  "Condition" : {

```

```
    "StringEquals" : {
      "aws:RequestTag/SSMForSAPCreated" : "True"
    }
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:*:iam:*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "PutMetricData",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage",
          "AWS/SSMForSAP"
        ]
      }
    }
  },
  {
    "Sid" : "CreateAttributeGroup",
    "Effect" : "Allow",
    "Action" : "servicecatalog:CreateAttributeGroup",
    "Resource" : "arn*:servicecatalog:*:*/attribute-groups/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/SSMForSAPCreated" : "True"
      }
    }
  },
  {
    "Sid" : "GetAttributeGroup",
```



```

    "Effect" : "Allow",
    "Action" : "servicecatalog:GetAttributeGroup",
    "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
  },
  {
    "Sid" : "DeleteAttributeGroup",
    "Effect" : "Allow",
    "Action" : "servicecatalog:DeleteAttributeGroup",
    "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/SSMForSAPCreated" : "True"
      }
    }
  },
  {
    "Sid" : "AttributeGroupActions",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:AssociateAttributeGroup",
      "servicecatalog:DisassociateAttributeGroup"
    ],
    "Resource" : "arn:*:servicecatalog:*:*:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/SSMForSAPCreated" : "True"
      }
    }
  },
  {
    "Sid" : "ListAssociatedAttributeGroups",
    "Effect" : "Allow",
    "Action" : "servicecatalog:ListAssociatedAttributeGroups",
    "Resource" : "arn:*:servicecatalog:*:*:*"
  },
  {
    "Sid" : "CreateGroup",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:Tag"
    ],
    "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
    "Condition" : {

```

```

    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "SSMForSAPCreated"
      ]
    }
  }
},
{
  "Sid" : "GetGroup",
  "Effect" : "Allow",
  "Action" : "resource-groups:GetGroup",
  "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
},
{
  "Sid" : "DeleteGroup",
  "Effect" : "Allow",
  "Action" : "resource-groups:DeleteGroup",
  "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "CreateAppTagResourceGroup",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:CreateGroup"
  ],
  "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
    }
  }
},
{
  "Sid" : "TagAppTagResourceGroup",
  "Effect" : "Allow",
  "Action" : [

```

```
    "resource-groups:Tag"
  ],
  "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
    }
  }
},
{
  "Sid" : "GetAppTagResourceGroupConfig",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:GetGroupConfiguration"
  ],
  "Resource" : [
    "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
  ]
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy est une [politique AWS gérée](#) qui : Stratégie pour le rôle lié à un service AWSServiceRoleForAmazonSSM_OpsInsights

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 16 juin 2021, 20:12 UTC
- Heure modifiée : 16 juin 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées](#)

AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator est une [politiqueAWS gérée](#) qui : Accès administrateur à l'annuaire SSO

Utilisation de la stratégie

Vous pouvez AWSSSODirectoryAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : politiqueAWS gérée
- Heure de création : 31 octobre 2018, 23:54 UTC
- Heure modifiée : 20 octobre 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Sid" : "AWSSSODirectoryAdministrator",
"Effect" : "Allow",
"Action" : [
  "sso-directory:*",
  "identitystore:*",
  "identitystore-auth:*",
  "sso:ListDirectoryAssociations"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly est une [politique AWS gérée](#) qui : ReadOnly accès à l'annuaire SSO

Utilisation de cette stratégie

Vous pouvez AWSSSODirectoryReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails de stratégie

- Type : politique AWS gérée
- Heure de création : 31 octobre 2018, 23:49 UTC
- Heure modifiée : 16 novembre 2022, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministrator est une [politique AWS gérée](#) qui : fournit un accès au sein du AWS SSO pour gérer les comptes AWS principaux et membres de l'organisation et les applications cloud

Utilisation de cette stratégie

Vous pouvez `AWSSSOMasterAccountAdministrator` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 juin 2018, 20:36 UTC
- Heure modifiée : 20 octobre 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "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"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSSSOManageDelegatedAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],

```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "sso.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator est une [politiqueAWS gérée](#) qui : fournit un accès au sein duAWS SSO pour gérer les comptes membres etAWS les applications cloud de l'Organizations

Utilisation de cette stratégie

Vous pouvez les associerAWSSSOMemberAccountAdministrator à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 juin 2018, 20:45 UTC
- Heure modifiée : 20 octobre 2022, 20:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "sso.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSOReadOnly

AWSSSOReadOnly est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux configurationsAWS SSO.

Utilisation de cette stratégie

Vous pouvezAWSSSOReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 juin 2018, 20:24 UTC
- Heure modifiée : 22 août 2022, 17:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

Version de la politique

Version de la politique :v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSSOServiceRolePolicy

AWSSSOServiceRolePolicy est une [politique AWS gérée](#) qui : accorde des autorisations AWS SSO pour gérer les AWS ressources, y compris les rôles IAM, les politiques et l'IdP SAML en votre nom.

Utilisation de de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des détails des détails

- Type : Politique de rôles liée à un service
- Heure de création : 5 décembre 2017, 18:36 UTC
- Heure modifiée : 20 octobre 2022, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Version de la politique

Version de la politique :v17 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
```

```

    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription",
    "iam:UpdateAssumeRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam>DeleteRolePermissionsBoundary"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "IAMRoleReadActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "IAMRoleCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteRole",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ]
},
{
  "Sid" : "IAMSLRCleanupActions",

```

```

    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:DeleteRole",
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
    ]
  },
  {
    "Sid" : "IAMSAMLProviderCreationAction",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateSAMLProvider"
    ],
    "Resource" : [
      "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ],
    "Condition" : {
      "StringNotEquals" : {
        "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "IAMSAMLProviderUpdateAction",
    "Effect" : "Allow",
    "Action" : [
      "iam:UpdateSAMLProvider"
    ],
    "Resource" : [
      "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
  },
  {
    "Sid" : "IAMSAMLProviderCleanupActions",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteSAMLProvider",
      "iam:GetSAMLProvider"
    ],
    "Resource" : [

```



```
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowUnauthAppForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:UnauthorizeApplication"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:DescribeDirectories",
    "ds:DescribeTrusts"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
  "Effect" : "Allow",
  "Action" : [
    "identitystore:DescribeUser",
    "identitystore:DescribeGroup",
    "identitystore:ListGroups",
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des des des des desAWS des autorisations de moindre privilège privilège privilège et évoluez et évoluez avec les autorisations de privilège](#)

AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess est une [politiqueAWS gérée](#) qui : Une politique d'accès permettant à un utilisateur/un rôle/etc. d'accéder à laAWS StepFunctions console. Pour profiter pleinement de la console, outre cette politique, un utilisateur peut avoir besoin de l'PassRole autorisation iam : pour d'autres rôles IAM pouvant être assumés par le service.

Utilisation de cette stratégie

Vous pouvezAWSStepFunctionsConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 janvier 2017, 21:54 UTC
- Heure modifiée : 12 janvier 2017, 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess` est une [politique AWS gérée](#) qui : Une politique d'accès permettant à un utilisateur/un rôle/etc. d'accéder à l'AWS StepFunctions API. Pour un accès complet, en plus de cette politique, un utilisateur DOIT disposer de l'`PassRole` autorisation `iam` : sur au moins un rôle IAM pouvant être assumé par le service.

Utilisation de cette stratégie

Vous pouvez les associer `AWSStepFunctionsFullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 janvier 2017, 21:51 UTC
- Heure modifiée : 11 janvier 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSStepFunctionsReadOnlyAccess

AWSStepFunctionsReadOnlyAccess est une [politiqueAWS gérée](#) qui : Une politique d'accès visant à fournir à un utilisateur/un rôle/etc. un accès en lecture seule auAWS StepFunctions service.

Utilisation de cette stratégie

Vous pouvezAWSStepFunctionsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 11 janvier 2017, 21:46 UTC
- Heure modifiée : 10 novembre 2017, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "states:ListStateMachines",
    "states:ListActivities",
    "states:DescribeStateMachine",
    "states:DescribeStateMachineForExecution",
    "states:ListExecutions",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:DescribeActivity"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSStorageGatewayFullAccess

AWSStorageGatewayFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AWS Storage Gateway via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AWSStorageGatewayFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 septembre 2022, 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSStorageGatewayReadOnlyAccess

AWSStorageGatewayReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès à AWS Storage Gateway via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez AWSStorageGatewayReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 septembre 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "fetchStorageGatewayParams",
    "Effect" : "Allow",
    "Action" : "ssm:GetParameters",
    "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSStorageGatewayServiceRolePolicy

AWSStorageGatewayServiceRolePolicy est une [politique AWS gérée](#) qui : Rôle lié à un service utilisé par AWS Storage Gateway pour permettre l'intégration d'autres AWS services à Storage Gateway.

Utilisation des politique de politique de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails des politique détails des

- Type : Politique de rôles liée à un service

- Heure de création : 17 février 2021, 19:03 UTC
- Heure modifiée : 17 février 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut des stratégie est la version qui définit les autorisations des stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie. Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document des stratégie Jpolitique Jpolitique

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des autorisations de moindre privilège deAWS moindre privilège de moindre privilège de moindre privilège de moindre privilège de politique de moindre privilège](#)

AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess est une [politique AWS gérée](#) qui :
AWSSupplyChainFederationAdminAccess fournit aux utilisateurs fédérés de la chaîne AWS d'approvisionnement un accès à l'application de chaîne AWS d'approvisionnement, y compris les autorisations requises pour effectuer des actions dans l'application de chaîne AWS d'approvisionnement. La politique fournit des autorisations administratives aux utilisateurs et aux groupes IAM Identity Center et est attachée à un rôle créé par AWS Supply Chain en votre nom. Vous ne devez associer AWSSupplyChainFederationAdminAccess de politique à aucune autre entité IAM.

Utilisation de cette politique

Vous pouvez vous associer AWSSupplyChainFederationAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 01 mars 2023, 18:54 UTC
- Heure modifiée : 1 novembre 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Sid" : "AWSSupplyChain",
    "Effect" : "Allow",
    "Action" : [
        "scn:*"
    ],
    "Resource" : [
        "arn:aws:scn:*:*:instance/*"
    ]
},
{
    "Sid" : "ChimeAppInstance",
    "Effect" : "Allow",
    "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime>DeleteChannelMembership",
        "chime>DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
    ],
    "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/SCNInstanceId" : "*"
        }
    }
},
{
    "Sid" : "ChimeChannel",

```

```
"Effect" : "Allow",
"Action" : [
  "chime:DescribeChannel"
],
"Resource" : [
  "arn:aws:chime:*:*:app-instance/*"
]
},
{
  "Sid" : "ChimeMessaging",
  "Effect" : "Allow",
  "Action" : [
    "chime:GetMessagingSessionEndpoint"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMIdentityCenter",
  "Effect" : "Allow",
  "Action" : [
    "sso:GetManagedApplicationInstance",
    "sso:ListDirectoryAssociations",
    "sso:AssociateProfile",
    "sso:DisassociateProfile",
    "sso:ListProfiles",
    "sso:GetProfile",
    "sso:ListProfileAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AppflowConnectorProfile",
  "Effect" : "Allow",
  "Action" : [
    "appflow:CreateConnectorProfile",
    "appflow:UseConnectorProfile",
    "appflow>DeleteConnectorProfile",
    "appflow:UpdateConnectorProfile"
  ],
  "Resource" : [
    "arn:aws:appflow:*:*:connectorprofile/scn-*"
  ]
},
{
```

```
"Sid" : "AppflowFlow",
"Effect" : "Allow",
"Action" : [
  "appflow:CreateFlow",
  "appflow>DeleteFlow",
  "appflow:DescribeFlow",
  "appflow:DescribeFlowExecutionRecords",
  "appflow:ListFlows",
  "appflow:StartFlow",
  "appflow:StopFlow",
  "appflow:UpdateFlow",
  "appflow:TagResource",
  "appflow:UntagResource"
],
"Resource" : [
  "arn:aws:appflow:*:*:flow/scn-*"
]
},
{
  "Sid" : "S3ListAllBuckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3ListSupplyChainBucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-supply-chain-data-*"
  ]
},
{
  "Sid" : "S3ReadWriteObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:s3::aws-supply-chain-data-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "SecretsManagerCreateSecret",
    "Effect" : "Allow",
    "Action" : "secretsmanager:CreateSecret",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:Name" : "appflow!*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "appflow.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "SecretsManagerPutResourcePolicy",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:PutResourcePolicy"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "appflow.amazonaws.com"
        ]
      },
      "StringEqualsIgnoreCase" : {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
      }
    }
  }
},
```

```
{
  "Sid" : "KMSListKeys",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Sid" : "KMSListGrants",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListGrants"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "appflow.*.amazonaws.com"
    },
    "StringEquals" : {
      "aws:ResourceTag/aws-supply-chain-access" : "true"
    }
  }
},
{
  "Sid" : "KMSCreateGrant",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "appflow.*.amazonaws.com"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringEquals" : {
      "aws:ResourceTag/aws-supply-chain-access" : "true"
    }
  }
}
```



```
}  
 ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSupportAccess

AWSSupportAccess est une [politique AWS gérée](#) qui : Autorise les utilisateurs à accéder au AWS Support Centre.

Utilisation de cette stratégie

Vous pouvez AWSSupportAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSupportAppFullAccess

AWSSupportAppFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à l'AWS Support application et aux autres services requis, tels que AWS Support les Service Quotas. Cette politique inclut les autorisations d'utilisation des services de support afin que l'utilisateur puisse contacter AWS Support pour des demandes d'assistance, modifier les quotas de service et créer les rôles liés aux services pertinents.

Utilisation de cette stratégie

Vous pouvez AWSSupportAppFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 22 août 2022, 16:53 UTC

- Heure modifiée : 22 août 2022, 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à l'AWS Supportapplication.

Utilisation de cette stratégie

Vous pouvezAWSSupportAppReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 22 août 2022, 17:01 UTC
- Heure modifiée : 22 août 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSupportPlansFullAccess

AWSSupportPlansFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux plans de support.

Utilisation de cette stratégie

Vous pouvez AWSSupportPlansFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 septembre 2022, 18:19 UTC
- Heure modifiée : 09 mai 2023, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSupportPlansReadOnlyAccess

AWSSupportPlansReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux plans de support.

Utilisation de cette stratégie

Vous pouvez `AWSSupportPlansReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 septembre 2022, 18:08 UTC
- Heure modifiée : 27 septembre 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSupportServiceRolePolicy

AWSSupportServiceRolePolicy est une [politique AWS gérée](#) qui : Permet d'accéder AWS Support aux AWS ressources pour fournir des services de facturation, d'administration et de support.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 19 avril 2018, 18:04 UTC
- Heure modifiée : 17 janvier 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Version de la politique

Version de la politique : v34 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
```



```

"Resource" : [
  "arn:aws:apigateway:*::/account",
  "arn:aws:apigateway:*::/apis",
  "arn:aws:apigateway:*::/apis/*",
  "arn:aws:apigateway:*::/apis/*/authorizers",
  "arn:aws:apigateway:*::/apis/*/authorizers/*",
  "arn:aws:apigateway:*::/apis/*/deployments",
  "arn:aws:apigateway:*::/apis/*/deployments/*",
  "arn:aws:apigateway:*::/apis/*/integrations",
  "arn:aws:apigateway:*::/apis/*/integrations/*",
  "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
  "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
  "arn:aws:apigateway:*::/apis/*/models",
  "arn:aws:apigateway:*::/apis/*/models/*",
  "arn:aws:apigateway:*::/apis/*/routes",
  "arn:aws:apigateway:*::/apis/*/routes/*",
  "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
  "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
  "arn:aws:apigateway:*::/apis/*/stages",
  "arn:aws:apigateway:*::/apis/*/stages/*",
  "arn:aws:apigateway:*::/clientcertificates",
  "arn:aws:apigateway:*::/clientcertificates/*",
  "arn:aws:apigateway:*::/domainnames",
  "arn:aws:apigateway:*::/domainnames/*",
  "arn:aws:apigateway:*::/domainnames/*/apimappings",
  "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
  "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
  "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
  "arn:aws:apigateway:*::/restapis",
  "arn:aws:apigateway:*::/restapis/*",
  "arn:aws:apigateway:*::/restapis/*/authorizers",
  "arn:aws:apigateway:*::/restapis/*/authorizers/*",
  "arn:aws:apigateway:*::/restapis/*/deployments",
  "arn:aws:apigateway:*::/restapis/*/deployments/*",
  "arn:aws:apigateway:*::/restapis/*/models",
  "arn:aws:apigateway:*::/restapis/*/models/*",
  "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
  "arn:aws:apigateway:*::/restapis/*/resources",
  "arn:aws:apigateway:*::/restapis/*/resources/*",
  "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
  "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
  "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
  "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",

```

```

    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/usageplans",
    "arn:aws:apigateway:*::/usageplans/*",
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Sid" : "AWSSupportDeleteRoleAccess",
  "Action" : [
    "iam:DeleteRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam:*::role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
  ]
},
{
  "Sid" : "AWSSupportActions",
  "Action" : [
    "access-analyzer:getAccessPreview",
    "access-analyzer:getAnalyzedResource",
    "access-analyzer:getAnalyzer",
    "access-analyzer:getArchiveRule",
    "access-analyzer:getFinding",
    "access-analyzer:getGeneratedPolicy",
    "access-analyzer:listAccessPreviewFindings",
    "access-analyzer:listAccessPreviews",
    "access-analyzer:listAnalyzedResources",
    "access-analyzer:listAnalyzers",
    "access-analyzer:listArchiveRules",
    "access-analyzer:listFindings",
    "access-analyzer:listPolicyGenerations",
    "acm-pca:describeCertificateAuthority",
    "acm-pca:describeCertificateAuthorityAuditReport",
    "acm-pca:getCertificate",
    "acm-pca:getCertificateAuthorityCertificate",
    "acm-pca:getCertificateAuthorityCsr",
    "acm-pca:listCertificateAuthorities",
    "acm-pca:listTags",
    "acm:describeCertificate",

```

```
"acm:getAccountConfiguration",
"acm:getCertificate",
"acm:listCertificates",
"acm:listTagsForCertificate",
"airflow:getEnvironment",
"airflow:listEnvironments",
"airflow:listTagsForResource",
"amplify:getApp",
"amplify:getBackendEnvironment",
"amplify:getBranch",
"amplify:getDomainAssociation",
"amplify:getJob",
"amplify:getWebhook",
"amplify:listApps",
"amplify:listBackendEnvironments",
"amplify:listBranches",
"amplify:listDomainAssociations",
"amplify:listWebhooks",
"amplifyuibuilder:exportComponents",
"amplifyuibuilder:exportThemes",
"appflow:describeConnectorEntity",
"appflow:describeConnectorProfiles",
"appflow:describeConnectors",
"appflow:describeFlow",
"appflow:describeFlowExecutionRecords",
"appflow:listConnectorEntities",
"appflow:listFlows",
"application-autoscaling:describeScalableTargets",
"application-autoscaling:describeScalingActivities",
"application-autoscaling:describeScalingPolicies",
"application-autoscaling:describeScheduledActions",
"applicationinsights:describeApplication",
"applicationinsights:describeComponent",
"applicationinsights:describeComponentConfiguration",
"applicationinsights:describeComponentConfigurationRecommendation",
"applicationinsights:describeLogPattern",
"applicationinsights:describeObservation",
"applicationinsights:describeProblem",
"applicationinsights:describeProblemObservations",
"applicationinsights:listApplications",
"applicationinsights:listComponents",
"applicationinsights:listConfigurationHistory",
"applicationinsights:listLogPatterns",
"applicationinsights:listLogPatternSets",
```

```
"applicationinsights:listProblems",
"appmesh:describeGatewayRoute",
"appmesh:describeMesh",
"appmesh:describeRoute",
"appmesh:describeVirtualGateway",
"appmesh:describeVirtualNode",
"appmesh:describeVirtualRouter",
"appmesh:describeVirtualService",
"appmesh:listGatewayRoutes",
"appmesh:listMeshes",
"appmesh:listRoutes",
"appmesh:listTagsForResource",
"appmesh:listVirtualGateways",
"appmesh:listVirtualNodes",
"appmesh:listVirtualRouters",
"appmesh:listVirtualServices",
"apprunner:describeAutoScalingConfiguration",
"apprunner:describeCustomDomains",
"apprunner:describeOperation",
"apprunner:describeService",
"apprunner:listAutoScalingConfigurations",
"apprunner:listConnections",
"apprunner:listOperations",
"apprunner:listServices",
"apprunner:listTagsForResource",
"appstream:describeAppBlockBuilderAppBlockAssociations",
"appstream:describeAppBlockBuilders",
"appstream:describeAppBlocks",
"appstream:describeApplicationFleetAssociations",
"appstream:describeApplications",
"appstream:describeDirectoryConfigs",
"appstream:describeEntitlements",
"appstream:describeFleets",
"appstream:describeImageBuilders",
"appstream:describeImagePermissions",
"appstream:describeImages",
"appstream:describeSessions",
"appstream:describeStacks",
"appstream:describeUsageReportSubscriptions",
"appstream:describeUsers",
"appstream:describeUserStackAssociations",
"appstream:listAssociatedFleets",
"appstream:listAssociatedStacks",
"appstream:listEntitledApplications",
```

```
"appstream:listTagsForResource",
"appsync:getApiAssociation",
"appsync:getApiCache",
"appsync:getDomainName",
"appsync:getFunction",
"appsync:getGraphQLApi",
"appsync:getIntrospectionSchema",
"appsync:getResolver",
"appsync:getSchemaCreationStatus",
"appsync:getSourceApiAssociation",
"appsync:getType",
"appsync:listDataSources",
"appsync:listDomainNames",
"appsync:listFunctions",
"appsync:listGraphQLApis",
"appsync:listResolvers",
"appsync:listResolversByFunction",
"appsync:listSourceApiAssociations",
"appsync:listTypes",
"appsync:listTypesByAssociation",
"aps:describeAlertManagerDefinition",
"aps:describeRuleGroupsNamespace",
"aps:describeWorkspace",
"aps:listRuleGroupsNamespaces",
"aps:listWorkspaces",
"athena:batchGetNamedQuery",
"athena:batchGetQueryExecution",
"athena:getCalculationExecution",
"athena:getCalculationExecutionStatus",
"athena:getDataCatalog",
"athena:getNamedQuery",
"athena:getNotebookMetadata",
"athena:getQueryExecution",
"athena:getQueryRuntimeStatistics",
"athena:getSession",
"athena:getSessionStatus",
"athena:getWorkGroup",
"athena:listApplicationDPUSizes",
"athena:listCalculationExecutions",
"athena:listDataCatalogs",
"athena:listEngineVersions",
"athena:listExecutors",
"athena:listNamedQueries",
"athena:listNotebookMetadata",
```

```
"athena:listNotebookSessions",
"athena:listQueryExecutions",
"athena:listSessions",
"athena:listTagsForResource",
"athena:listWorkGroups",
"auditmanager:getAccountStatus",
"auditmanager:getDelegations",
"auditmanager:listAssessmentFrameworks",
"auditmanager:listAssessmentReports",
"auditmanager:listAssessments",
"auditmanager:listControls",
"auditmanager:listKeywordsForDataSource",
"auditmanager:listNotifications",
"autoscaling-plans:describeScalingPlanResources",
"autoscaling-plans:describeScalingPlans",
"autoscaling-plans:getScalingPlanResourceForecastData",
"autoscaling:describeAccountLimits",
"autoscaling:describeAdjustmentTypes",
"autoscaling:describeAutoScalingGroups",
"autoscaling:describeAutoScalingInstances",
"autoscaling:describeAutoScalingNotificationTypes",
"autoscaling:describeInstanceRefreshes",
"autoscaling:describeLaunchConfigurations",
"autoscaling:describeLifecycleHooks",
"autoscaling:describeLifecycleHookTypes",
"autoscaling:describeLoadBalancers",
"autoscaling:describeLoadBalancerTargetGroups",
"autoscaling:describeMetricCollectionTypes",
"autoscaling:describeNotificationConfigurations",
"autoscaling:describePolicies",
"autoscaling:describeScalingActivities",
"autoscaling:describeScalingProcessTypes",
"autoscaling:describeScheduledActions",
"autoscaling:describeTags",
"autoscaling:describeTerminationPolicyTypes",
"autoscaling:describeWarmPool",
"backup:describeBackupJob",
"backup:describeBackupVault",
"backup:describeCopyJob",
"backup:describeFramework",
"backup:describeGlobalSettings",
"backup:describeProtectedResource",
"backup:describeRecoveryPoint",
"backup:describeRegionSettings",
```

```
"backup:describeReportJob",
"backup:describeReportPlan",
"backup:describeRestoreJob",
"backup:getBackupPlan",
"backup:getBackupPlanFromJSON",
"backup:getBackupPlanFromTemplate",
"backup:getBackupSelection",
"backup:getBackupVaultAccessPolicy",
"backup:getBackupVaultNotifications",
"backup:getLegalHold",
"backup:getRecoveryPointRestoreMetadata",
"backup:getSupportedResourceTypes",
"backup:listBackupJobs",
"backup:listBackupPlans",
"backup:listBackupPlanTemplates",
"backup:listBackupPlanVersions",
"backup:listBackupSelections",
"backup:listBackupVaults",
"backup:listCopyJobs",
"backup:listFrameworks",
"backup:listLegalHolds",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup:listTags",
"backup-gateway:getGateway",
"backup-gateway:getHypervisor",
"backup-gateway:getHypervisorPropertyMappings",
"backup-gateway:getVirtualMachine",
"backup-gateway:listGateways",
"backup-gateway:listHypervisors",
"backup-gateway:listVirtualMachines",
"batch:describeComputeEnvironments",
"batch:describeJobDefinitions",
"batch:describeJobQueues",
"batch:describeJobs",
"batch:listJobs",
"braket:getDevice",
"braket:getQuantumTask",
"braket:searchDevices",
```

```
"braket:searchQuantumTasks",
"budgets:viewBudget",
"ce:getCostAndUsage",
"ce:getCostAndUsageWithResources",
"ce:getCostForecast",
"ce:getDimensionValues",
"ce:getReservationCoverage",
"ce:getReservationPurchaseRecommendation",
"ce:getReservationUtilization",
"ce:getRightsizingRecommendation",
"ce:getSavingsPlansCoverage",
"ce:getSavingsPlansPurchaseRecommendation",
"ce:getSavingsPlansUtilization",
"ce:getSavingsPlansUtilizationDetails",
"ce:getTags",
"chime:describeAppInstance",
"chime:getAttendee",
"chime:getGlobalSettings",
"chime:getMediaCapturePipeline",
"chime:getMediaPipeline",
"chime:getMeeting",
"chime:getProxySession",
"chime:getSipMediaApplication",
"chime:getSipRule",
"chime:getVoiceConnector",
"chime:getVoiceConnectorGroup",
"chime:getVoiceConnectorLoggingConfiguration",
"chime:listAppInstances",
"chime:listAttendees",
"chime:listChannelBans",
"chime:listChannels",
"chime:listChannelsModeratedByAppInstanceUser",
"chime:listMediaCapturePipelines",
"chime:listMediaPipelines",
"chime:listMeetings",
"chime:listSipMediaApplications",
"chime:listSipRules",
"chime:listVoiceConnectorGroups",
"chime:listVoiceConnectors",
"cleanrooms:batchGetCollaborationAnalysisTemplate",
"cleanrooms:batchGetSchema",
"cleanrooms:getAnalysisTemplate",
"cleanrooms:getCollaboration",
"cleanrooms:getCollaborationAnalysisTemplate",
```



```
"cleanrooms:getConfiguredTable",
"cleanrooms:getConfiguredTableAssociation",
"cleanrooms:getMembership",
"cleanrooms:getSchema",
"cleanrooms:listAnalysisTemplates",
"cleanrooms:listCollaborationAnalysisTemplates",
"cleanrooms:listCollaborations",
"cleanrooms:listConfiguredTableAssociations",
"cleanrooms:listConfiguredTables",
"cleanrooms:listMembers",
"cleanrooms:listMemberships",
"cleanrooms:listSchemas",
"cloud9:describeEnvironmentMemberships",
"cloud9:describeEnvironments",
"cloud9:listEnvironments",
"clouddirectory:getDirectory",
"clouddirectory:listDirectories",
"cloudformation:batchDescribeTypeConfigurations",
"cloudformation:describeAccountLimits",
"cloudformation:describeChangeSet",
"cloudformation:describeChangeSetHooks",
"cloudformation:describePublisher",
"cloudformation:describeStackEvents",
"cloudformation:describeStackInstance",
"cloudformation:describeStackResource",
"cloudformation:describeStackResources",
"cloudformation:describeStacks",
"cloudformation:describeStackSet",
"cloudformation:describeStackSetOperation",
"cloudformation:describeType",
"cloudformation:describeTypeRegistration",
"cloudformation:estimateTemplateCost",
"cloudformation:getStackPolicy",
"cloudformation:getTemplate",
"cloudformation:getTemplateSummary",
"cloudformation:listChangeSets",
"cloudformation:listExports",
"cloudformation:listImports",
"cloudformation:listStackInstances",
"cloudformation:listStackResources",
"cloudformation:listStacks",
"cloudformation:listStackSetOperationResults",
"cloudformation:listStackSetOperations",
"cloudformation:listStackSets",
```

```
"cloudformation:listTypeRegistrations",
"cloudformation:listTypes",
"cloudformation:listTypeVersions",
"cloudfront:describeFunction",
"cloudfront:getCachePolicy",
"cloudfront:getCachePolicyConfig",
"cloudfront:getCloudFrontOriginAccessIdentity",
"cloudfront:getCloudFrontOriginAccessIdentityConfig",
"cloudfront:getContinuousDeploymentPolicy",
"cloudfront:getContinuousDeploymentPolicyConfig",
"cloudfront:getDistribution",
"cloudfront:getDistributionConfig",
"cloudfront:getInvalidation",
"cloudfront:getKeyGroup",
"cloudfront:getKeyGroupConfig",
"cloudfront:getMonitoringSubscription",
"cloudfront:getOriginAccessControl",
"cloudfront:getOriginAccessControlConfig",
"cloudfront:getOriginRequestPolicy",
"cloudfront:getOriginRequestPolicyConfig",
"cloudfront:getPublicKey",
"cloudfront:getPublicKeyConfig",
"cloudfront:getRealtimeLogConfig",
"cloudfront:getStreamingDistribution",
"cloudfront:getStreamingDistributionConfig",
"cloudfront:listCachePolicies",
"cloudfront:listCloudFrontOriginAccessIdentities",
"cloudfront:listContinuousDeploymentPolicies",
"cloudfront:listDistributions",
"cloudfront:listDistributionsByCachePolicyId",
"cloudfront:listDistributionsByKeyGroup",
"cloudfront:listDistributionsByOriginRequestPolicyId",
"cloudfront:listDistributionsByRealtimeLogConfig",
"cloudfront:listDistributionsByResponseHeadersPolicyId",
"cloudfront:listDistributionsByWebACLId",
"cloudfront:listFunctions",
"cloudfront:listInvalidations",
"cloudfront:listKeyGroups",
"cloudfront:listOriginAccessControls",
"cloudfront:listOriginRequestPolicies",
"cloudfront:listPublicKeys",
"cloudfront:listRealtimeLogConfigs",
"cloudfront:listStreamingDistributions",
"cloudhsm:describeBackups",
```

```
"cloudhsm:describeClusters",
"cloudsearch:describeAnalysisSchemes",
"cloudsearch:describeAvailabilityOptions",
"cloudsearch:describeDomains",
"cloudsearch:describeExpressions",
"cloudsearch:describeIndexFields",
"cloudsearch:describeScalingParameters",
"cloudsearch:describeServiceAccessPolicies",
"cloudsearch:describeSuggesters",
"cloudsearch:listDomainNames",
"cloudtrail:describeTrails",
"cloudtrail:getEventSelectors",
"cloudtrail:getInsightSelectors",
"cloudtrail:getTrail",
"cloudtrail:getTrailStatus",
"cloudtrail:listPublicKeys",
"cloudtrail:listTags",
"cloudtrail:listTrails",
"cloudtrail:lookupEvents",
"cloudwatch:describeAlarmHistory",
"cloudwatch:describeAlarms",
"cloudwatch:describeAlarmsForMetric",
"cloudwatch:describeAnomalyDetectors",
"cloudwatch:describeInsightRules",
"cloudwatch:getDashboard",
"cloudwatch:getInsightRuleReport",
"cloudwatch:getMetricData",
"cloudwatch:getMetricStatistics",
"cloudwatch:getMetricStream",
"cloudwatch:listDashboards",
"cloudwatch:listManagedInsightRules",
"cloudwatch:listMetrics",
"cloudwatch:listMetricStreams",
"codeartifact:describeDomain",
"codeartifact:describePackageVersion",
"codeartifact:describeRepository",
"codeartifact:getDomainPermissionsPolicy",
"codeartifact:getRepositoryEndpoint",
"codeartifact:getRepositoryPermissionsPolicy",
"codeartifact:listDomains",
"codeartifact:listPackages",
"codeartifact:listPackageVersionAssets",
"codeartifact:listPackageVersions",
"codeartifact:listRepositories",
```

```
"codeartifact:listRepositoriesInDomain",
"codebuild:batchGetBuildBatches",
"codebuild:batchGetBuilds",
"codebuild:batchGetProjects",
"codebuild:listBuildBatches",
"codebuild:listBuildBatchesForProject",
"codebuild:listBuilds",
"codebuild:listBuildsForProject",
"codebuild:listCuratedEnvironmentImages",
"codebuild:listProjects",
"codebuild:listSourceCredentials",
"codecommit:batchGetRepositories",
"codecommit:getBranch",
"codecommit:getRepository",
"codecommit:getRepositoryTriggers",
"codecommit:listBranches",
"codecommit:listRepositories",
"codedeploy:batchGetApplicationRevisions",
"codedeploy:batchGetApplications",
"codedeploy:batchGetDeploymentGroups",
"codedeploy:batchGetDeploymentInstances",
"codedeploy:batchGetDeployments",
"codedeploy:batchGetDeploymentTargets",
"codedeploy:batchGetOnPremisesInstances",
"codedeploy:getApplication",
"codedeploy:getApplicationRevision",
"codedeploy:getDeployment",
"codedeploy:getDeploymentConfig",
"codedeploy:getDeploymentGroup",
"codedeploy:getDeploymentInstance",
"codedeploy:getDeploymentTarget",
"codedeploy:getOnPremisesInstance",
"codedeploy:listApplicationRevisions",
"codedeploy:listApplications",
"codedeploy:listDeploymentConfigs",
"codedeploy:listDeploymentGroups",
"codedeploy:listDeploymentInstances",
"codedeploy:listDeployments",
"codedeploy:listDeploymentTargets",
"codedeploy:listGitHubAccountTokenNames",
"codedeploy:listOnPremisesInstances",
"codepipeline:getJobDetails",
"codepipeline:getPipeline",
"codepipeline:getPipelineExecution",
```

```
"codepipeline:getPipelineState",
"codepipeline:listActionExecutions",
"codepipeline:listActionTypes",
"codepipeline:listPipelineExecutions",
"codepipeline:listPipelines",
"codepipeline:listWebhooks",
"codestar:describeProject",
"codestar:listProjects",
"codestar:listResources",
"codestar:listTeamMembers",
"codestar:listUserProfiles",
"codestar-connections:getConnection",
"codestar-connections:getHost",
"codestar-connections:listConnections",
"codestar-connections:listHosts",
"cognito-identity:describeIdentityPool",
"cognito-identity:getIdentityPoolRoles",
"cognito-identity:listIdentities",
"cognito-identity:listIdentityPools",
"cognito-idp:describeIdentityProvider",
"cognito-idp:describeResourceServer",
"cognito-idp:describeRiskConfiguration",
"cognito-idp:describeUserImportJob",
"cognito-idp:describeUserPool",
"cognito-idp:describeUserPoolClient",
"cognito-idp:describeUserPoolDomain",
"cognito-idp:getGroup",
"cognito-idp:getUICustomization",
"cognito-idp:getUserPoolMfaConfig",
"cognito-idp:listGroups",
"cognito-idp:listIdentityProviders",
"cognito-idp:listResourceServers",
"cognito-idp:listUserImportJobs",
"cognito-idp:listUserPoolClients",
"cognito-idp:listUserPools",
"cognito-sync:describeDataset",
"cognito-sync:describeIdentityPoolUsage",
"cognito-sync:describeIdentityUsage",
"cognito-sync:getCognitoEvents",
"cognito-sync:getIdentityPoolConfiguration",
"cognito-sync:listDatasets",
"cognito-sync:listIdentityPoolUsage",
"comprehend:describeDocumentClassificationJob",
"comprehend:describeDocumentClassifier",
```

```
"comprehend:describeDominantLanguageDetectionJob",
"comprehend:describeEndpoint",
"comprehend:describeEntitiesDetectionJob",
"comprehend:describeEntityRecognizer",
"comprehend:describeEventsDetectionJob",
"comprehend:describeFlywheel",
"comprehend:describeFlywheelIteration",
"comprehend:describeKeyPhrasesDetectionJob",
"comprehend:describePiiEntitiesDetectionJob",
"comprehend:describeSentimentDetectionJob",
"comprehend:describeTargetedSentimentDetectionJob",
"comprehend:describeTopicsDetectionJob",
"comprehend:listDocumentClassificationJobs",
"comprehend:listDocumentClassifiers",
"comprehend:listDominantLanguageDetectionJobs",
"comprehend:listEndpoints",
"comprehend:listEntitiesDetectionJobs",
"comprehend:listEntityRecognizers",
"comprehend:listEventsDetectionJobs",
"comprehend:listFlywheelIterationHistory",
"comprehend:listFlywheels",
"comprehend:listKeyPhrasesDetectionJobs",
"comprehend:listPiiEntitiesDetectionJobs",
"comprehend:listSentimentDetectionJobs",
"comprehend:listTargetedSentimentDetectionJobs",
"comprehend:listTopicsDetectionJobs",
"compute-optimizer:getAutoScalingGroupRecommendations",
"compute-optimizer:getEBSVolumeRecommendations",
"compute-optimizer:getEC2InstanceRecommendations",
"compute-optimizer:getEC2RecommendationProjectedMetrics",
"compute-optimizer:getECSServiceRecommendations",
"compute-optimizer:getECSServiceRecommendationProjectedMetrics",
"compute-optimizer:getEnrollmentStatus",
"compute-optimizer:getRecommendationSummaries",
"config:batchGetAggregateResourceConfig",
"config:batchGetResourceConfig",
"config:describeAggregateComplianceByConfigRules",
"config:describeAggregationAuthorizations",
"config:describeComplianceByConfigRule",
"config:describeComplianceByResource",
"config:describeConfigRuleEvaluationStatus",
"config:describeConfigRules",
"config:describeConfigurationAggregators",
"config:describeConfigurationAggregatorSourcesStatus",
```

```
"config:describeConfigurationRecorders",
"config:describeConfigurationRecorderStatus",
"config:describeConformancePackCompliance",
"config:describeConformancePacks",
"config:describeConformancePackStatus",
"config:describeDeliveryChannels",
"config:describeDeliveryChannelStatus",
"config:describeOrganizationConfigRules",
"config:describeOrganizationConfigRuleStatuses",
"config:describeOrganizationConformancePacks",
"config:describeOrganizationConformancePackStatuses",
"config:describePendingAggregationRequests",
"config:describeRemediationConfigurations",
"config:describeRemediationExceptions",
"config:describeRemediationExecutionStatus",
"config:describeRetentionConfigurations",
"config:getAggregateComplianceDetailsByConfigRule",
"config:getAggregateConfigRuleComplianceSummary",
"config:getAggregateDiscoveredResourceCounts",
"config:getAggregateResourceConfig",
"config:getComplianceDetailsByConfigRule",
"config:getComplianceDetailsByResource",
"config:getComplianceSummaryByConfigRule",
"config:getComplianceSummaryByResourceType",
"config:getConformancePackComplianceDetails",
"config:getConformancePackComplianceSummary",
"config:getDiscoveredResourceCounts",
"config:getOrganizationConfigRuleDetailedStatus",
"config:getOrganizationConformancePackDetailedStatus",
"config:getResourceConfigHistory",
"config:listAggregateDiscoveredResources",
"config:listDiscoveredResources",
"config:listTagsForResource",
"connect:describeContact",
"connect:describePhoneNumber",
"connect:describeQuickConnect",
"connect:describeUser",
"connect:getCurrentMetricData",
"connect:getMetricData",
"connect:listContactEvaluations",
"connect:listEvaluationForms",
"connect:listEvaluationFormVersions",
"connect:listPhoneNumbersV2",
"connect:listQuickConnects",
```

```
"connect:listRoutingProfiles",
"connect:listSecurityProfiles",
"connect:listUsers",
"connect:listViews",
"connect:listViewVersions",
"controltower:describeAccountFactoryConfig",
"controltower:describeCoreService",
"controltower:describeGuardrail",
"controltower:describeGuardrailForTarget",
"controltower:describeManagedAccount",
"controltower:describeSingleSignOn",
"controltower:getAvailableUpdates",
"controltower:getHomeRegion",
"controltower:getLandingZoneStatus",
"controltower:listDirectoryGroups",
"controltower:listGuardrailsForTarget",
"controltower:listGuardrailViolations",
"controltower:listManagedAccounts",
"controltower:listManagedAccountsForGuardrail",
"controltower:listManagedAccountsForParent",
"controltower:listManagedOrganizationalUnits",
"controltower:listManagedOrganizationalUnitsForGuardrail",
"databrew:describeDataset",
"databrew:describeJob",
"databrew:describeProject",
"databrew:describeRecipe",
"databrew:listDatasets",
"databrew:listJobRuns",
"databrew:listJobs",
"databrew:listProjects",
"databrew:listRecipes",
"databrew:listRecipeVersions",
"databrew:listTagsForResource",
"datapipeline:describeObjects",
"datapipeline:describePipelines",
"datapipeline:getPipelineDefinition",
"datapipeline:listPipelines",
"datapipeline:queryObjects",
"datasync:describeAgent",
"datasync:describeLocationEfs",
"datasync:describeLocationFsxLustre",
"datasync:describeLocationFsxOpenZfs",
"datasync:describeLocationFsxWindows",
"datasync:describeLocationHdfs",
```



```
"datasync:describeLocationNfs",
"datasync:describeLocationObjectStorage",
"datasync:describeLocationS3",
"datasync:describeLocationSmb",
"datasync:describeTask",
"datasync:describeTaskExecution",
"datasync:listAgents",
"datasync:listLocations",
"datasync:listTaskExecutions",
"datasync:listTasks",
"dax:describeClusters",
"dax:describeDefaultParameters",
"dax:describeEvents",
"dax:describeParameterGroups",
"dax:describeParameters",
"dax:describeSubnetGroups",
"detective:getMembers",
"detective:listGraphs",
"detective:listInvitations",
"detective:listMembers",
"devicefarm:getAccountSettings",
"devicefarm:getDevice",
"devicefarm:getDevicePool",
"devicefarm:getDevicePoolCompatibility",
"devicefarm:getJob",
"devicefarm:getProject",
"devicefarm:getRemoteAccessSession",
"devicefarm:getRun",
"devicefarm:getSuite",
"devicefarm:getTest",
"devicefarm:getTestGridProject",
"devicefarm:getTestGridSession",
"devicefarm:getUpload",
"devicefarm:listArtifacts",
"devicefarm:listDevicePools",
"devicefarm:listDevices",
"devicefarm:listJobs",
"devicefarm:listProjects",
"devicefarm:listRemoteAccessSessions",
"devicefarm:listRuns",
"devicefarm:listSamples",
"devicefarm:listSuites",
"devicefarm:listTestGridProjects",
"devicefarm:listTestGridSessionActions",
```

```
"devicefarm:listTestGridSessionArtifacts",
"devicefarm:listTestGridSessions",
"devicefarm:listTests",
"devicefarm:listUniqueProblems",
"devicefarm:listUploads",
"directconnect:describeConnectionLoa",
"directconnect:describeConnections",
"directconnect:describeConnectionsOnInterconnect",
"directconnect:describeCustomerMetadata",
"directconnect:describeDirectConnectGatewayAssociationProposals",
"directconnect:describeDirectConnectGatewayAssociations",
"directconnect:describeDirectConnectGatewayAttachments",
"directconnect:describeDirectConnectGateways",
"directconnect:describeHostedConnections",
"directconnect:describeInterconnectLoa",
"directconnect:describeInterconnects",
"directconnect:describeLags",
"directconnect:describeLoa",
"directconnect:describeLocations",
"directconnect:describeRouterConfiguration",
"directconnect:describeVirtualGateways",
"directconnect:describeVirtualInterfaces",
"dms:getLifecyclePolicies",
"dms:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
```

```
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
"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:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"ec2:describeIpams",
"ec2:describeIpamScopes",
"ec2:describeIpv6Pools",
"ec2:describeKeyPairs",
"ec2:describeLaunchTemplates",
"ec2:describeLaunchTemplateVersions",
"ec2:describeLocalGatewayRouteTables",
"ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:describeLocalGatewayRouteTableVpcAssociations",
"ec2:describeLocalGateways",
"ec2:describeLocalGatewayVirtualInterfaceGroups",
"ec2:describeLocalGatewayVirtualInterfaces",
"ec2:describeManagedPrefixLists",
"ec2:describeMovingAddresses",
"ec2:describeNatGateways",
"ec2:describeNetworkAcls",
"ec2:describeNetworkInterfaceAttribute",
"ec2:describeNetworkInterfaces",
"ec2:describePlacementGroups",
"ec2:describePrefixLists",
"ec2:describePrincipalIdFormat",
"ec2:describePublicIpv4Pools",
"ec2:describeRegions",
"ec2:describeReservedInstances",
```

```
"ec2:describeReservedInstancesListings",
"ec2:describeReservedInstancesModifications",
"ec2:describeReservedInstancesOfferings",
"ec2:describeRouteTables",
"ec2:describeScheduledInstanceAvailability",
"ec2:describeScheduledInstances",
"ec2:describeSecurityGroupReferences",
"ec2:describeSecurityGroupRules",
"ec2:describeSecurityGroups",
"ec2:describeSnapshotAttribute",
"ec2:describeSnapshots",
"ec2:describeSpotDatafeedSubscription",
"ec2:describeSpotFleetInstances",
"ec2:describeSpotFleetRequestHistory",
"ec2:describeSpotFleetRequests",
"ec2:describeSpotInstanceRequests",
"ec2:describeSpotPriceHistory",
"ec2:describeStaleSecurityGroups",
"ec2:describeStoreImageTasks",
"ec2:describeSubnets",
"ec2:describeTags",
"ec2:describeTrafficMirrorFilters",
"ec2:describeTrafficMirrorSessions",
"ec2:describeTrafficMirrorTargets",
"ec2:describeTransitGatewayAttachments",
"ec2:describeTransitGatewayConnectPeers",
"ec2:describeTransitGatewayMulticastDomains",
"ec2:describeTransitGatewayPeeringAttachments",
"ec2:describeTransitGatewayPolicyTables",
"ec2:describeTransitGatewayRouteTableAnnouncements",
"ec2:describeTransitGatewayRouteTables",
"ec2:describeTransitGateways",
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"ec2:describeVpcAttribute",
"ec2:describeVpcClassicLink",
"ec2:describeVpcClassicLinkDnsSupport",
```

```
"ec2:describeVpcEndpointConnectionNotifications",
"ec2:describeVpcEndpointConnections",
"ec2:describeVpcEndpoints",
"ec2:describeVpcEndpointServiceConfigurations",
"ec2:describeVpcEndpointServicePermissions",
"ec2:describeVpcEndpointServices",
"ec2:describeVpcPeeringConnections",
"ec2:describeVpcs",
"ec2:describeVpnConnections",
"ec2:describeVpnGateways",
"ec2:getAssociatedIpv6PoolCidrs",
"ec2:getCapacityReservationUsage",
"ec2:getCoipPoolUsage",
"ec2:getConsoleOutput",
"ec2:getConsoleScreenshot",
"ec2:getDefaultCreditSpecification",
"ec2:getEbsDefaultKmsKeyId",
"ec2:getEbsEncryptionByDefault",
"ec2:getGroupsForCapacityReservation",
"ec2:getHostReservationPurchasePreview",
"ec2:getInstanceTypesFromInstanceRequirements",
"ec2:getIpamAddressHistory",
"ec2:getIpamPoolAllocations",
"ec2:getIpamPoolCidrs",
"ec2:getIpamResourceCidrs",
"ec2:getLaunchTemplateData",
"ec2:getManagedPrefixListAssociations",
"ec2:getManagedPrefixListEntries",
"ec2:getReservedInstancesExchangeQuote",
"ec2:getSerialConsoleAccessStatus",
"ec2:getSpotPlacementScores",
"ec2:getTransitGatewayMulticastDomainAssociations",
"ec2:getTransitGatewayPrefixListReferences",
"ec2:getVerifiedAccessEndpointPolicy",
"ec2:getVerifiedAccessGroupPolicy",
"ec2:listImagesInRecycleBin",
"ec2:listSnapshotsInRecycleBin",
"ec2:searchLocalGatewayRoutes",
"ec2:searchTransitGatewayMulticastGroups",
"ec2:searchTransitGatewayRoutes",
"ecr-public:describeImages",
"ecr-public:describeImageTags",
"ecr-public:describeRegistries",
"ecr-public:describeRepositories",
```

```
"ecr-public:getRegistryCatalogData",
"ecr-public:getRepositoryCatalogData",
"ecr-public:getRepositoryPolicy",
"ecr-public:listTagsForResource",
"ecr:batchCheckLayerAvailability",
"ecr:batchGetRepositoryScanningConfiguration",
"ecr:describeImages",
"ecr:describeImageReplicationStatus",
"ecr:describeImageScanFindings",
"ecr:describePullThroughCacheRules",
"ecr:describeRegistry",
"ecr:describeRepositories",
"ecr:getLifecyclePolicy",
"ecr:getLifecyclePolicyPreview",
"ecr:getRegistryPolicy",
"ecr:getRegistryScanningConfiguration",
"ecr:getRepositoryPolicy",
"ecr:listImages",
"ecr:listTagsForResource",
"ecs:describeCapacityProviders",
"ecs:describeClusters",
"ecs:describeContainerInstances",
"ecs:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"ecs:getTaskProtection",
"ecs:listAccountSettings",
"ecs:listAttributes",
"ecs:listClusters",
"ecs:listContainerInstances",
"ecs:listServices",
"ecs:listServicesByNamespace",
"ecs:listTagsForResource",
"ecs:listTaskDefinitionFamilies",
"ecs:listTaskDefinitions",
"ecs:listTasks",
"eks:describeAccessEntry",
"eks:describeAddon",
"eks:describeAddonConfiguration",
"eks:describeAddonVersions",
"eks:describeCluster",
"eks:describeEksAnywhereSubscription",
"eks:describeFargateProfile",
```



```
"eks:describeIdentityProviderConfig",
"eks:describeNodegroup",
"eks:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"eks:listUpdates",
"elasticache:describeCacheClusters",
"elasticache:describeCacheEngineVersions",
"elasticache:describeCacheParameterGroups",
"elasticache:describeCacheParameters",
"elasticache:describeCacheSecurityGroups",
"elasticache:describeCacheSubnetGroups",
"elasticache:describeEngineDefaultParameters",
"elasticache:describeEvents",
"elasticache:describeGlobalReplicationGroups",
"elasticache:describeReplicationGroups",
"elasticache:describeReservedCacheNodes",
"elasticache:describeReservedCacheNodesOfferings",
"elasticache:describeServerlessCaches",
"elasticache:describeServerlessCacheSnapshots",
"elasticache:describeServiceUpdates",
"elasticache:describeSnapshots",
"elasticache:describeUpdateActions",
"elasticache:describeUserGroups",
"elasticache:describeUsers",
"elasticache:listAllowedNodeTypeModifications",
"elasticache:listTagsForResource",
"elasticbeanstalk:checkDNSAvailability",
"elasticbeanstalk:describeAccountAttributes",
"elasticbeanstalk:describeApplicationVersions",
"elasticbeanstalk:describeApplications",
"elasticbeanstalk:describeConfigurationOptions",
"elasticbeanstalk:describeEnvironmentHealth",
"elasticbeanstalk:describeEnvironmentManagedActionHistory",
"elasticbeanstalk:describeEnvironmentManagedActions",
"elasticbeanstalk:describeEnvironmentResources",
"elasticbeanstalk:describeEnvironments",
```

```
"elasticbeanstalk:describeEvents",
"elasticbeanstalk:describeInstancesHealth",
"elasticbeanstalk:describePlatformVersion",
"elasticbeanstalk:listAvailableSolutionStacks",
"elasticbeanstalk:listPlatformBranches",
"elasticbeanstalk:listPlatformVersions",
"elasticbeanstalk:validateConfigurationSettings",
"elasticfilesystem:describeAccessPoints",
"elasticfilesystem:describeFileSystemPolicy",
"elasticfilesystem:describeFileSystems",
"elasticfilesystem:describeLifecycleConfiguration",
"elasticfilesystem:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"elasticfilesystem:describeTags",
"elasticfilesystem:listTagsForResource",
"elasticloadbalancing:describeAccountLimits",
"elasticloadbalancing:describeInstanceHealth",
"elasticloadbalancing:describeListenerCertificates",
"elasticloadbalancing:describeListeners",
"elasticloadbalancing:describeLoadBalancerAttributes",
"elasticloadbalancing:describeLoadBalancerPolicies",
"elasticloadbalancing:describeLoadBalancerPolicyTypes",
"elasticloadbalancing:describeLoadBalancers",
"elasticloadbalancing:describeRules",
"elasticloadbalancing:describeSSLPolicies",
"elasticloadbalancing:describeTags",
"elasticloadbalancing:describeTargetGroupAttributes",
"elasticloadbalancing:describeTargetGroups",
"elasticloadbalancing:describeTargetHealth",
"elasticmapreduce:describeCluster",
"elasticmapreduce:describeNotebookExecution",
"elasticmapreduce:describeReleaseLabel",
"elasticmapreduce:describeSecurityConfiguration",
"elasticmapreduce:describeStep",
"elasticmapreduce:describeStudio",
"elasticmapreduce:getAutoTerminationPolicy",
"elasticmapreduce:getBlockPublicAccessConfiguration",
"elasticmapreduce:getManagedScalingPolicy",
"elasticmapreduce:getStudioSessionMapping",
"elasticmapreduce:listBootstrapActions",
"elasticmapreduce:listClusters",
"elasticmapreduce:listInstanceFleets",
"elasticmapreduce:listInstanceGroups",
"elasticmapreduce:listInstances",
```

```
"elasticmapreduce:listNotebookExecutions",
"elasticmapreduce:listReleaseLabels",
"elasticmapreduce:listSecurityConfigurations",
"elasticmapreduce:listSteps",
"elasticmapreduce:listStudios",
"elasticmapreduce:listStudioSessionMappings",
"elastictranscoder:listJobsByPipeline",
"elastictranscoder:listJobsByStatus",
"elastictranscoder:listPipelines",
"elastictranscoder:listPresets",
"elastictranscoder:readPipeline",
"elastictranscoder:readPreset",
"emr-containers:describeJobRun",
"emr-containers:describeJobTemplate",
"emr-containers:describeManagedEndpoint",
"emr-containers:describeVirtualCluster",
"emr-containers:listJobRuns",
"emr-containers:listJobTemplates",
"emr-containers:listManagedEndpoints",
"emr-containers:listVirtualClusters",
"emr-serverless:getApplication",
"emr-serverless:getJobRun",
"emr-serverless:listApplications",
"es:describeDomain",
"es:describeDomainAutoTunes",
"es:describeDomainChangeProgress",
"es:describeDomainConfig",
"es:describeDomains",
"es:describeDryRunProgress",
"es:describeElasticsearchDomain",
"es:describeElasticsearchDomainConfig",
"es:describeElasticsearchDomains",
"es:describeInboundConnections",
"es:describeInstanceTypeLimits",
"es:describeOutboundConnections",
"es:describePackages",
"es:describeReservedInstanceOfferings",
"es:describeReservedInstances",
"es:describeVpcEndpoints",
"es:getCompatibleVersions",
"es:getPackageVersionHistory",
"es:getUpgradeHistory",
"es:getUpgradeStatus",
"es:listDomainNames",
```

```
"es:listDomainsForPackage",
"es:listInstanceTypeDetails",
"es:listPackagesForDomain",
"es:listScheduledActions",
"es:listTags",
"es:listVersions",
"es:listVpcEndpointAccess",
"es:listVpcEndpoints",
"es:listVpcEndpointsForDomain",
"evidently:getExperiment",
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
```

```
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
"fms:listPolicies",
"forecast:describeDataset",
"forecast:describeDatasetGroup",
"forecast:describeDatasetImportJob",
"forecast:describeForecast",
"forecast:describeForecastExportJob",
"forecast:describePredictor",
"forecast:getAccuracyMetrics",
"forecast:listDatasetGroups",
"forecast:listDatasetImportJobs",
"forecast:listDatasets",
"forecast:listForecastExportJobs",
"forecast:listForecasts",
"forecast:listPredictors",
"fsx:describeBackups",
"fsx:describeDataRepositoryAssociations",
"fsx:describeDataRepositoryTasks",
"fsx:describeFileCaches",
"fsx:describeFileSystems",
"fsx:describeSnapshots",
"fsx:describeStorageVirtualMachines",
"fsx:describeVolumes",
"fsx:listTagsForResource",
"gamelift:describeAlias",
"gamelift:describeBuild",
"gamelift:describeEC2InstanceLimits",
"gamelift:describeFleetAttributes",
"gamelift:describeFleetCapacity",
"gamelift:describeFleetEvents",
"gamelift:describeFleetLocationAttributes",
"gamelift:describeFleetLocationCapacity",
"gamelift:describeFleetLocationUtilization",
"gamelift:describeFleetPortSettings",
"gamelift:describeFleetUtilization",
"gamelift:describeGameServer",
"gamelift:describeGameServerGroup",
"gamelift:describeGameSessionDetails",
```

```
"gamelift:describeGameSessionPlacement",
"gamelift:describeGameSessionQueues",
"gamelift:describeGameSessions",
"gamelift:describeInstances",
"gamelift:describeMatchmaking",
"gamelift:describeMatchmakingConfigurations",
"gamelift:describeMatchmakingRuleSets",
"gamelift:describePlayerSessions",
"gamelift:describeRuntimeConfiguration",
"gamelift:describeScalingPolicies",
"gamelift:describeScript",
"gamelift:listAliases",
"gamelift:listBuilds",
"gamelift:listFleets",
"gamelift:listGameServerGroups",
"gamelift:listGameServers",
"gamelift:listScripts",
"gamelift:resolveAlias",
"glacier:describeJob",
"glacier:describeVault",
"glacier:getDataRetrievalPolicy",
"glacier:getVaultAccessPolicy",
"glacier:getVaultLock",
"glacier:getVaultNotifications",
"glacier:listJobs",
"glacier:listTagsForVault",
"glacier:listVaults",
"globalaccelerator:describeAccelerator",
"globalaccelerator:describeAcceleratorAttributes",
"globalaccelerator:describeEndpointGroup",
"globalaccelerator:describeListener",
"globalaccelerator:listAccelerators",
"globalaccelerator:listEndpointGroups",
"globalaccelerator:listListeners",
"glue:batchGetBlueprints",
"glue:batchGetCrawlers",
"glue:batchGetDevEndpoints",
"glue:batchGetJobs",
"glue:batchGetPartition",
"glue:batchGetTriggers",
"glue:batchGetWorkflows",
"glue:checkSchemaVersionValidity",
"glue:getBlueprint",
"glue:getBlueprintRun",
```

```
"glue:getBlueprintRuns",
"glue:getCatalogImportStatus",
"glue:getClassifier",
"glue:getClassifiers",
"glue:getColumnStatisticsForPartition",
"glue:getColumnStatisticsForTable",
"glue:getCrawler",
"glue:getCrawlerMetrics",
"glue:getCrawlers",
"glue:getCustomEntityType",
"glue:getDatabase",
"glue:getDatabases",
"glue:getDataflowGraph",
"glue:getDataQualityResult",
"glue:getDataQualityRuleRecommendationRun",
"glue:getDataQualityRuleset",
"glue:getDataQualityRulesetEvaluationRun",
"glue:getDevEndpoint",
"glue:getDevEndpoints",
"glue:getJob",
"glue:getJobRun",
"glue:getJobRuns",
"glue:getJobs",
"glue:getMapping",
"glue:getMLTaskRun",
"glue:getMLTaskRuns",
"glue:getMLTransform",
"glue:getMLTransforms",
"glue:getPartition",
"glue:getPartitionIndexes",
"glue:getPartitions",
"glue:getRegistry",
"glue:getResourcePolicies",
"glue:getResourcePolicy",
"glue:getSchema",
"glue:getSchemaByDefinition",
"glue:getSchemaVersion",
"glue:getSchemaVersionsDiff",
"glue:getSession",
"glue:getStatement",
"glue:getTable",
"glue:getTables",
"glue:getTableVersions",
"glue:getTrigger",
```

```
"glue:getTriggers",
"glue:getUserDefinedFunction",
"glue:getUserDefinedFunctions",
"glue:getWorkflow",
"glue:getWorkflowRun",
"glue:getWorkflowRuns",
"glue:listCrawlers",
"glue:listCrawls",
"glue:listDataQualityResults",
"glue:listDataQualityRuleRecommendationRuns",
"glue:listDataQualityRulesetEvaluationRuns",
"glue:listDataQualityRulesets",
"glue:listDevEndpoints",
"glue:listMLTransforms",
"glue:listRegistries",
"glue:listSchemas",
"glue:listSchemaVersions",
"glue:listSessions",
"glue:listStatements",
"glue:querySchemaVersionMetadata",
"greengrass:getConnectivityInfo",
"greengrass:getCoreDefinition",
"greengrass:getCoreDefinitionVersion",
"greengrass:getDeploymentStatus",
"greengrass:getDeviceDefinition",
"greengrass:getDeviceDefinitionVersion",
"greengrass:getFunctionDefinition",
"greengrass:getFunctionDefinitionVersion",
"greengrass:getGroup",
"greengrass:getGroupCertificateAuthority",
"greengrass:getGroupVersion",
"greengrass:getLoggerDefinition",
"greengrass:getLoggerDefinitionVersion",
"greengrass:getResourceDefinitionVersion",
"greengrass:getServiceRoleForAccount",
"greengrass:getSubscriptionDefinition",
"greengrass:getSubscriptionDefinitionVersion",
"greengrass:listCoreDefinitions",
"greengrass:listCoreDefinitionVersions",
"greengrass:listDeployments",
"greengrass:listDeviceDefinitions",
"greengrass:listDeviceDefinitionVersions",
"greengrass:listFunctionDefinitions",
"greengrass:listFunctionDefinitionVersions",
```



```
"greengrass:listGroups",
"greengrass:listGroupVersions",
"greengrass:listLoggerDefinitions",
"greengrass:listLoggerDefinitionVersions",
"greengrass:listResourceDefinitions",
"greengrass:listResourceDefinitionVersions",
"greengrass:listSubscriptionDefinitions",
"greengrass:listSubscriptionDefinitionVersions",
"guardduty:getDetector",
"guardduty:getFindings",
"guardduty:getFindingsStatistics",
"guardduty:getInvitationsCount",
"guardduty:getIPSet",
"guardduty:getMasterAccount",
"guardduty:getMembers",
"guardduty:getThreatIntelSet",
"guardduty:listDetectors",
"guardduty:listFindings",
"guardduty:listInvitations",
"guardduty:listIPSets",
"guardduty:listMembers",
"guardduty:listThreatIntelSets",
"health:describeAffectedAccountsForOrganization",
"health:describeAffectedEntities",
"health:describeAffectedEntitiesForOrganization",
"health:describeEntityAggregates",
"health:describeEntityAggregatesForOrganization",
"health:describeEventAggregates",
"health:describeEventDetails",
"health:describeEventDetailsForOrganization",
"health:describeEvents",
"health:describeEventsForOrganization",
"health:describeEventTypes",
"health:describeHealthServiceStatusForOrganization",
"iam:getAccessKeyLastUsed",
"iam:getAccountAuthorizationDetails",
"iam:getAccountPasswordPolicy",
"iam:getAccountSummary",
"iam:getContextKeysForCustomPolicy",
"iam:getContextKeysForPrincipalPolicy",
"iam:getCredentialReport",
"iam:getGroup",
"iam:getGroupPolicy",
"iam:getInstanceProfile",
```

```
"iam:getLoginProfile",
"iam:getOpenIDConnectProvider",
"iam:getPolicy",
"iam:getPolicyVersion",
"iam:getRole",
"iam:getRolePolicy",
"iam:getSAMLProvider",
"iam:getServerCertificate",
"iam:getServiceLinkedRoleDeletionStatus",
"iam:getSSHPublicKey",
"iam:getUser",
"iam:getUserPolicy",
"iam:listAccessKeys",
"iam:listAccountAliases",
"iam:listAttachedGroupPolicies",
"iam:listAttachedRolePolicies",
"iam:listAttachedUserPolicies",
"iam:listEntitiesForPolicy",
"iam:listGroupPolicies",
"iam:listGroups",
"iam:listGroupsForUser",
"iam:listInstanceProfiles",
"iam:listInstanceProfilesForRole",
"iam:listMFADevices",
"iam:listOpenIDConnectProviders",
"iam:listPolicies",
"iam:listPolicyVersions",
"iam:listRolePolicies",
"iam:listRoles",
"iam:listSAMLProviders",
"iam:listServerCertificates",
"iam:listSigningCertificates",
"iam:listSSHPublicKeys",
"iam:listUserPolicies",
"iam:listUsers",
"iam:listVirtualMFADevices",
"iam:simulateCustomPolicy",
"iam:simulatePrincipalPolicy",
"imagebuilder:getComponent",
"imagebuilder:getComponentPolicy",
"imagebuilder:getContainerRecipe",
"imagebuilder:getDistributionConfiguration",
"imagebuilder:getImage",
"imagebuilder:getImagePipeline",
```

```
"imagebuilder:getImagePolicy",
"imagebuilder:getImageRecipe",
"imagebuilder:getImageRecipePolicy",
"imagebuilder:getInfrastructureConfiguration",
"imagebuilder:getLifecycleExecution",
"imagebuilder:getLifecyclePolicy",
"imagebuilder:getWorkflowExecution",
"imagebuilder:getWorkflowStepExecution",
"imagebuilder:listComponentBuildVersions",
"imagebuilder:listComponents",
"imagebuilder:listContainerRecipes",
"imagebuilder:listDistributionConfigurations",
"imagebuilder:listImageBuildVersions",
"imagebuilder:listImagePipelineImages",
"imagebuilder:listImagePipelines",
"imagebuilder:listImageRecipes",
"imagebuilder:listImages",
"imagebuilder:listImageScanFindingAggregations",
"imagebuilder:listInfrastructureConfigurations",
"imagebuilder:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflowStepExecutions",
"imagebuilder:listTagsForResource",
"inspector:describeAssessmentRuns",
"inspector:describeAssessmentTargets",
"inspector:describeAssessmentTemplates",
"inspector:describeCrossAccountAccessRole",
"inspector:describeResourceGroups",
"inspector:describeRulesPackages",
"inspector:getTelemetryMetadata",
"inspector:listAssessmentRunAgents",
"inspector:listAssessmentRuns",
"inspector:listAssessmentTargets",
"inspector:listAssessmentTemplates",
"inspector:listEventSubscriptions",
"inspector:listRulesPackages",
"inspector:listTagsForResource",
"inspector2:batchGetAccountStatus",
"inspector2:batchGetFreeTrialInfo",
"inspector2:describeOrganizationConfiguration",
"inspector2:getDelegatedAdminAccount",
"inspector2:getMember",
```

```
"inspector2:getSbomExport",
"inspector2:listCoverage",
"inspector2:listDelegatedAdminAccounts",
"inspector2:listFilters",
"inspector2:listFindings",
"inspector2:listMembers",
"inspector2:listUsageTotals",
"inspector-scan:scanSbom",
"internetmonitor:getMonitor",
"internetmonitor:listMonitors",
"internetmonitor:getHealthEvent",
"internetmonitor:listHealthEvents",
"iot:describeAuthorizer",
"iot:describeCACertificate",
"iot:describeCertificate",
"iot:describeDefaultAuthorizer",
"iot:describeDomainConfiguration",
"iot:describeEndpoint",
"iot:describeIndex",
"iot:describeJobExecution",
"iot:describeThing",
"iot:describeThingGroup",
"iot:describeTunnel",
"iot:getEffectivePolicies",
"iot:getIndexingConfiguration",
"iot:getLoggingOptions",
"iot:getPolicy",
"iot:getPolicyVersion",
"iot:getTopicRule",
"iot:getV2LoggingOptions",
"iot:listAttachedPolicies",
"iot:listAuthorizers",
"iot:listCACertificates",
"iot:listCertificates",
"iot:listCertificatesByCA",
"iot:listDomainConfigurations",
"iot:listJobExecutionsForJob",
"iot:listJobExecutionsForThing",
"iot:listJobs",
"iot:listNamedShadowsForThing",
"iot:listOutgoingCertificates",
"iot:listPackages",
"iot:listPackageVersions",
"iot:listPolicies",
```

```
"iot:listPolicyPrincipals",
"iot:listPolicyVersions",
"iot:listPrincipalPolicies",
"iot:listPrincipalThings",
"iot:listRoleAliases",
"iot:listTargetsForPolicy",
"iot:listThingGroups",
"iot:listThingGroupsForThing",
"iot:listThingPrincipals",
"iot:listThingRegistrationTasks",
"iot:listThings",
"iot:listThingsInThingGroup",
"iot:listThingTypes",
"iot:listTopicRules",
"iot:listTunnels",
"iot:listV2LoggingLevels",
"iotevents:describeDetector",
"iotevents:describeDetectorModel",
"iotevents:describeInput",
"iotevents:describeLoggingOptions",
"iotevents:listDetectorModels",
"iotevents:listDetectorModelVersions",
"iotevents:listDetectors",
"iotevents:listInputs",
"iotfleetwise:getCampaign",
"iotfleetwise:getDecoderManifest",
"iotfleetwise:getFleet",
"iotfleetwise:getModelManifest",
"iotfleetwise:getSignalCatalog",
"iotfleetwise:getVehicle",
"iotfleetwise:getVehicleStatus",
"iotfleetwise:listCampaigns",
"iotfleetwise:listDecoderManifests",
"iotfleetwise:listDecoderManifestNetworkInterfaces",
"iotfleetwise:listDecoderManifestSignals",
"iotfleetwise:listFleets",
"iotfleetwise:listFleetsForVehicle",
"iotfleetwise:listModelManifests",
"iotfleetwise:listModelManifestNodes",
"iotfleetwise:listSignalCatalogs",
"iotfleetwise:listSignalCatalogNodes",
"iotfleetwise:listVehicles",
"iotsitewise:describeAccessPolicy",
"iotsitewise:describeAsset",
```

```
"iotsitewise:describeAssetModel",
"iotsitewise:describeAssetProperty",
"iotsitewise:describeDashboard",
"iotsitewise:describeGateway",
"iotsitewise:describeGatewayCapabilityConfiguration",
"iotsitewise:describeLoggingOptions",
"iotsitewise:describePortal",
"iotsitewise:describeProject",
"iotsitewise:listAccessPolicies",
"iotsitewise:listAssetModels",
"iotsitewise:listAssets",
"iotsitewise:listAssociatedAssets",
"iotsitewise:listDashboards",
"iotsitewise:listGateways",
"iotsitewise:listPortals",
"iotsitewise:listProjectAssets",
"iotsitewise:listProjects",
"iottwinmaker:getComponentType",
"iottwinmaker:getEntity",
"iottwinmaker:getPricingPlan",
"iottwinmaker:getScene",
"iottwinmaker:getWorkspace",
"iottwinmaker:listComponentTypes",
"iottwinmaker:listEntities",
"iottwinmaker:listScenes",
"iottwinmaker:getSyncJob",
"iottwinmaker:listSyncJobs",
"iottwinmaker:listSyncResources",
"iottwinmaker:listWorkspaces",
"iotwireless:getDestination",
"iotwireless:getDeviceProfile",
"iotwireless:getPartnerAccount",
"iotwireless:getServiceEndpoint",
"iotwireless:getServiceProfile",
"iotwireless:getWirelessDevice",
"iotwireless:getWirelessDeviceStatistics",
"iotwireless:getWirelessGateway",
"iotwireless:getWirelessGatewayCertificate",
"iotwireless:getWirelessGatewayFirmwareInformation",
"iotwireless:getWirelessGatewayStatistics",
"iotwireless:getWirelessGatewayTask",
"iotwireless:getWirelessGatewayTaskDefinition",
"iotwireless:listDestinations",
"iotwireless:listDeviceProfiles",
```

```
"iotwireless:listPartnerAccounts",
"iotwireless:listServiceProfiles",
"iotwireless:listTagsForResource",
"iotwireless:listWirelessDevices",
"iotwireless:listWirelessGateways",
"iotwireless:listWirelessGatewayTaskDefinitions",
"ivs:getChannel",
"ivs:getRecordingConfiguration",
"ivs:getStream",
"ivs:getStreamSession",
"ivs:listChannels",
"ivs:listPlaybackKeyPairs",
"ivs:listRecordingConfigurations",
"ivs:listStreamKeys",
"ivs:listStreams",
"ivs:listStreamSessions",
"kafka:describeCluster",
"kafka:describeClusterOperation",
"kafka:describeClusterV2",
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:getBootstrapBrokers",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClusterOperations",
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"kafkaconnect:describeConnector",
"kafkaconnect:describeCustomPlugin",
"kafkaconnect:describeWorkerConfiguration",
"kafkaconnect:listConnectors",
"kafkaconnect:listCustomPlugins",
"kafkaconnect:listWorkerConfigurations",
"kendra:describeDataSource",
"kendra:describeFaq",
"kendra:describeIndex",
"kendra:listDataSources",
"kendra:listFaqs",
"kendra:listIndices",
"kinesis:describeStream",
"kinesis:describeStreamConsumer",
"kinesis:describeStreamSummary",
"kinesis:listShards",
```

```
"kinesis:listStreams",
"kinesis:listStreamConsumers",
"kinesis:listTagsForStream",
"kinesisanalytics:describeApplication",
"kinesisanalytics:describeApplicationSnapshot",
"kinesisanalytics:listApplications",
"kinesisanalytics:listApplicationSnapshots",
"kinesisvideo:describeImageGenerationConfiguration",
"kinesisvideo:describeNotificationConfiguration",
"kinesisvideo:describeSignalingChannel",
"kinesisvideo:describeStream",
"kinesisvideo:getDataEndpoint",
"kinesisvideo:getIceServerConfig",
"kinesisvideo:getSignalingChannelEndpoint",
"kinesisvideo:listSignalingChannels",
"kinesisvideo:listStreams",
"kms:describeKey",
"kms:getKeyPolicy",
"kms:getKeyRotationStatus",
"kms:listAliases",
"kms:listGrants",
"kms:listKeyPolicies",
"kms:listKeys",
"kms:listResourceTags",
"kms:listRetirableGrants",
"lambda:getAccountSettings",
"lambda:getAlias",
"lambda:getCodeSigningConfig",
"lambda:getEventSourceMapping",
"lambda:getFunction",
"lambda:getFunctionCodeSigningConfig",
"lambda:getFunctionConcurrency",
"lambda:getFunctionConfiguration",
"lambda:getFunctionEventInvokeConfig",
"lambda:getFunctionUrlConfig",
"lambda:getLayerVersion",
"lambda:getLayerVersionPolicy",
"lambda:getPolicy",
"lambda:getProvisionedConcurrencyConfig",
"lambda:getRuntimeManagementConfig",
"lambda:listAliases",
"lambda:listCodeSigningConfigs",
"lambda:listEventSourceMappings",
"lambda:listFunctionEventInvokeConfigs",
```



```
"lambda:listFunctions",
"lambda:listFunctionsByCodeSigningConfig",
"lambda:listFunctionUrlConfigs",
"lambda:listLayers",
"lambda:listLayerVersions",
"lambda:listProvisionedConcurrencyConfigs",
"lambda:listVersionsByFunction",
"launchwizard:describeProvisionedApp",
"launchwizard:describeProvisioningEvents",
"launchwizard:listProvisionedApps",
"lex:describeBot",
"lex:describeBotAlias",
"lex:describeBotLocale",
"lex:describeBotRecommendation",
"lex:describeBotVersion",
"lex:describeCustomVocabularyMetadata",
"lex:describeExport",
"lex:describeImport",
"lex:describeIntent",
"lex:describeResourcePolicy",
"lex:describeSlot",
"lex:describeSlotType",
"lex:getBot",
"lex:getBotAlias",
"lex:getBotAliases",
"lex:getBotChannelAssociation",
"lex:getBotChannelAssociations",
"lex:getBots",
"lex:getBotVersions",
"lex:getBuiltinIntent",
"lex:getBuiltinIntents",
"lex:getBuiltinSlotTypes",
"lex:getIntent",
"lex:getIntents",
"lex:getIntentVersions",
"lex:getSlotType",
"lex:getSlotTypes",
"lex:getSlotTypeVersions",
"lex:listBotAliases",
"lex:listBotLocales",
"lex:listBotRecommendations",
"lex:listBots",
"lex:listBotVersions",
"lex:listExports",
```

```
"lex:listImports",
"lex:listIntents",
"lex:listRecommendedIntents",
"lex:listSlots",
"lex:listSlotTypes",
"license-manager:getLicenseConfiguration",
"license-manager:getServiceSettings",
"license-manager:listAssociationsForLicenseConfiguration",
"license-manager:listFailuresForLicenseConfigurationOperations",
"license-manager:listLicenseConfigurations",
"license-manager:listLicenseSpecificationsForResource",
"license-manager:listResourceInventory",
"license-manager:listUsageForLicenseConfiguration",
"lightsail:getActiveNames",
"lightsail:getAlarms",
"lightsail:getAutoSnapshots",
"lightsail:getBlueprints",
"lightsail:getBucketBundles",
"lightsail:getBucketMetricData",
"lightsail:getBuckets",
"lightsail:getBundles",
"lightsail:getCertificates",
"lightsail:getContainerImages",
"lightsail:getContainerServiceDeployments",
"lightsail:getContainerServiceMetricData",
"lightsail:getContainerServicePowers",
"lightsail:getContainerServices",
"lightsail:getDisk",
"lightsail:getDisks",
"lightsail:getDiskSnapshot",
"lightsail:getDiskSnapshots",
"lightsail:getDistributionBundles",
"lightsail:getDistributionMetricData",
"lightsail:getDistributions",
"lightsail:getDomain",
"lightsail:getDomains",
"lightsail:getExportSnapshotRecords",
"lightsail:getInstance",
"lightsail:getInstanceMetricData",
"lightsail:getInstancePortStates",
"lightsail:getInstances",
"lightsail:getInstanceSnapshot",
"lightsail:getInstanceSnapshots",
"lightsail:getInstanceState",
```

```
"lightsail:getKeyPair",
"lightsail:getKeyPairs",
"lightsail:getLoadBalancer",
"lightsail:getLoadBalancerMetricData",
"lightsail:getLoadBalancers",
"lightsail:getLoadBalancerTlsCertificates",
"lightsail:getOperation",
"lightsail:getOperations",
"lightsail:getOperationsForResource",
"lightsail:getRegions",
"lightsail:getRelationalDatabase",
"lightsail:getRelationalDatabaseMetricData",
"lightsail:getRelationalDatabases",
"lightsail:getRelationalDatabaseSnapshot",
"lightsail:getRelationalDatabaseSnapshots",
"lightsail:getStaticIp",
"lightsail:getStaticIps",
"lightsail:isVpcPeered",
"logs:describeAccountPolicies",
"logs:describeDeliveries",
"logs:describeDeliveryDestinations",
"logs:describeDeliverySources",
"logs:describeDestinations",
"logs:describeExportTasks",
"logs:describeLogGroups",
"logs:describeLogStreams",
"logs:describeMetricFilters",
"logs:describeQueries",
"logs:describeQueryDefinitions",
"logs:describeResourcePolicies",
"logs:describeSubscriptionFilters",
"logs:getDataProtectionPolicy",
"logs:getDelivery",
"logs:getDeliveryDestination",
"logs:getDeliveryDestinationPolicy",
"logs:getDeliverySource",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listLogDeliveries",
"logs:testMetricFilter",
"lookoutequipment:describeDataIngestionJob",
"lookoutequipment:describeDataset",
"lookoutequipment:describeInferenceScheduler",
"lookoutequipment:describeModel",
```

```
"lookoutequipment:listDataIngestionJobs",
"lookoutequipment:listDatasets",
"lookoutequipment:listInferenceExecutions",
"lookoutequipment:listInferenceSchedulers",
"lookoutequipment:listModels",
"lookoutmetrics:describeAlert",
"lookoutmetrics:describeAnomalyDetectionExecutions",
"lookoutmetrics:describeAnomalyDetector",
"lookoutmetrics:describeMetricSet",
"lookoutmetrics:getAnomalyGroup",
"lookoutmetrics:getDataQualityMetrics",
"lookoutmetrics:getFeedback",
"lookoutmetrics:getSampleData",
"lookoutmetrics:listAlerts",
"lookoutmetrics:listAnomalyDetectors",
"lookoutmetrics:listAnomalyGroupSummaries",
"lookoutmetrics:listAnomalyGroupTimeSeries",
"lookoutmetrics:listMetricSets",
"lookoutmetrics:listTagsForResource",
"machinelearning:describeBatchPredictions",
"machinelearning:describeDataSources",
"machinelearning:describeEvaluations",
"machinelearning:describeMLModels",
"machinelearning:getBatchPrediction",
"machinelearning:getDataSource",
"machinelearning:getEvaluation",
"machinelearning:getMLModel",
"macie2:getClassificationExportConfiguration",
"macie2:getCustomDataIdentifier",
"macie2:getFindings",
"macie2:getFindingStatistics",
"macie2:listClassificationJobs",
"macie2:listCustomDataIdentifiers",
"macie2:listFindings",
"managedblockchain:getMember",
"managedblockchain:getNetwork",
"managedblockchain:getNode",
"managedblockchain:listMembers",
"managedblockchain:listNetworks",
"managedblockchain:listNodes",
"mediaconnect:describeFlow",
"mediaconnect:listEntitlements",
"mediaconnect:listFlows",
"mediaconvert:describeEndpoints",
```

```
"mediaconvert:getJob",
"mediaconvert:getJobTemplate",
"mediaconvert:getPreset",
"mediaconvert:getQueue",
"mediaconvert:listJobs",
"mediaconvert:listJobTemplates",
"medialive:describeChannel",
"medialive:describeInput",
"medialive:describeInputDevice",
"medialive:describeInputSecurityGroup",
"medialive:describeMultiplex",
"medialive:describeOffering",
"medialive:describeReservation",
"medialive:describeSchedule",
"medialive:listChannels",
"medialive:listInputDevices",
"medialive:listInputs",
"medialive:listInputSecurityGroups",
"medialive:listMultiplexes",
"medialive:listOfferings",
"medialive:listReservations",
"mediapackage:describeChannel",
"mediapackage:describeOriginEndpoint",
"mediapackage:listChannels",
"mediapackage:listOriginEndpoints",
"mediastore:describeContainer",
"mediastore:getContainerPolicy",
"mediastore:getCorsPolicy",
"mediastore:listContainers",
"mediatailor:getPlaybackConfiguration",
"mediatailor:listPlaybackConfigurations",
"medical-imaging:getDatastore",
"medical-imaging:listDatastores",
"mgn:describeJobLogItems",
"mgn:describeJobs",
"mgn:describeLaunchConfigurationTemplates",
"mgn:describeReplicationConfigurationTemplates",
"mgn:describeSourceServers",
"mgn:describeVcenterClients",
"mgn:getLaunchConfiguration",
"mgn:getReplicationConfiguration",
"mgn:listApplications",
"mgn:listSourceServerActions",
"mgn:listTemplateActions",
```

```
"mgn:listWaves",
"mobiletargeting:getAdmChannel",
"mobiletargeting:getApnsChannel",
"mobiletargeting:getApnsSandboxChannel",
"mobiletargeting:getApnsVoipChannel",
"mobiletargeting:getApnsVoipSandboxChannel",
"mobiletargeting:getApp",
"mobiletargeting:getApplicationSettings",
"mobiletargeting:getApps",
"mobiletargeting:getBaiduChannel",
"mobiletargeting:getCampaign",
"mobiletargeting:getCampaignActivities",
"mobiletargeting:getCampaigns",
"mobiletargeting:getCampaignVersion",
"mobiletargeting:getCampaignVersions",
"mobiletargeting:getEmailChannel",
"mobiletargeting:getEndpoint",
"mobiletargeting:getEventStream",
"mobiletargeting:getExportJob",
"mobiletargeting:getExportJobs",
"mobiletargeting:getGcmChannel",
"mobiletargeting:getImportJob",
"mobiletargeting:getImportJobs",
"mobiletargeting:getJourney",
"mobiletargeting:getJourneyExecutionMetrics",
"mobiletargeting:getJourneyExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionMetrics",
"mobiletargeting:getJourneyRuns",
"mobiletargeting:getSegment",
"mobiletargeting:getSegmentImportJobs",
"mobiletargeting:getSegments",
"mobiletargeting:getSegmentVersion",
"mobiletargeting:getSegmentVersions",
"mobiletargeting:getSmsChannel",
"mobiletargeting:listJourneys",
"mq:describeBroker",
"mq:describeConfiguration",
"mq:describeConfigurationRevision",
"mq:describeUser",
"mq:listBrokers",
"mq:listConfigurationRevisions",
"mq:listConfigurations",
"mq:listUsers",
```

```
"m2:getApplication",
"m2:getApplicationVersion",
"m2:getBatchJobExecution",
"m2:getDataSetDetails",
"m2:getDataSetImportTask",
"m2:getDeployment",
"m2:getEnvironment",
"m2:listApplications",
"m2:listApplicationVersions",
"m2:listBatchJobDefinitions",
"m2:listBatchJobExecutions",
"m2:listDataSetImportHistory",
"m2:listDataSets",
"m2:listDeployments",
"m2:listEngineVersions",
"m2:listEnvironments",
"network-firewall:describeFirewall",
"network-firewall:describeFirewallPolicy",
"network-firewall:describeLoggingConfiguration",
"network-firewall:describeRuleGroup",
"network-firewall:describeTlsInspectionConfiguration",
"network-firewall:listFirewallPolicies",
"network-firewall:listFirewalls",
"network-firewall:listRuleGroups",
"network-firewall:listTlsInspectionConfigurations",
"networkmanager:describeGlobalNetworks",
"networkmanager:getConnectAttachment",
"networkmanager:getConnections",
"networkmanager:getConnectPeer",
"networkmanager:getConnectPeerAssociations",
"networkmanager:getCoreNetwork",
"networkmanager:getCoreNetworkChangeEvents",
"networkmanager:getCoreNetworkChangeSet",
"networkmanager:getCoreNetworkPolicy",
"networkmanager:getCustomerGatewayAssociations",
"networkmanager:getDevices",
"networkmanager:getLinkAssociations",
"networkmanager:getLinks",
"networkmanager:getNetworkResourceCounts",
"networkmanager:getNetworkResourceRelationships",
"networkmanager:getNetworkResources",
"networkmanager:getNetworkRoutes",
"networkmanager:getNetworkTelemetry",
"networkmanager:getResourcePolicy",
```

```
"networkmanager:getRouteAnalysis",
"networkmanager:getSites",
"networkmanager:getSiteToSiteVpnAttachment",
"networkmanager:getTransitGatewayConnectPeerAssociations",
"networkmanager:getTransitGatewayPeering",
"networkmanager:getTransitGatewayRegistrations",
"networkmanager:getTransitGatewayRouteTableAttachment",
"networkmanager:getVpcAttachment",
"networkmanager:listAttachments",
"networkmanager:listConnectPeers",
"networkmanager:listCoreNetworkPolicyVersions",
"networkmanager:listCoreNetworks",
"networkmanager:listOrganizationServiceAccessStatus",
"networkmanager:listPeerings",
"networkmanager:listTagsForResource",
"nimble:getEula",
"nimble:getLaunchProfile",
"nimble:getLaunchProfileDetails",
"nimble:getLaunchProfileInitialization",
"nimble:getLaunchProfileMember",
"nimble:getStreamingImage",
"nimble:getStreamingSession",
"nimble:getStreamingSessionStream",
"nimble:getStudio",
"nimble:getStudioComponent",
"nimble:listEulaAcceptances",
"nimble:listEulas",
"nimble:listLaunchProfiles",
"nimble:listStreamingImages",
"nimble:listStreamingSessions",
"nimble:listStudioComponents",
"nimble:listStudios",
"notifications:getEventRule",
"notifications:getNotificationConfiguration",
"notifications:getNotificationEvent",
"notifications:listChannels",
"notifications:listEventRules",
"notifications:listNotificationConfigurations",
"notifications:listNotificationEvents",
"notifications:listNotificationHubs",
"notifications-contacts:getEmailContact",
"notifications-contacts:listEmailContacts",
"oam:getLink",
"oam:getSink",
```



```
"oam:getSinkPolicy",
"oam:listAttachedLinks",
"oam:listLinks",
"oam:listSinks",
"omics:getAnnotationImportJob",
"omics:getAnnotationStore",
"omics:getReadSetImportJob",
"omics:getReadSetMetadata",
"omics:getReference",
"omics:getReferenceImportJob",
"omics:getReferenceMetadata",
"omics:getReferenceStore",
"omics:getRun",
"omics:getRunGroup",
"omics:getSequenceStore",
"omics:getVariantImportJob",
"omics:getVariantStore",
"omics:getWorkflow",
"omics:listAnnotationImportJobs",
"omics:listAnnotationStores",
"omics:listMultipartReadSetUploads",
"omics:listReadSetImportJobs",
"omics:listReadSets",
"omics:listReadSetUploadParts",
"omics:listReferenceImportJobs",
"omics:listReferenceStores",
"omics:listReferences",
"omics:listRunGroups",
"omics:listRunTasks",
"omics:listRuns",
"omics:listSequenceStores",
"omics:listVariantImportJobs",
"omics:listVariantStores",
"omics:listWorkflows",
"opsworks-cm:describeAccountAttributes",
"opsworks-cm:describeBackups",
"opsworks-cm:describeEvents",
"opsworks-cm:describeNodeAssociationStatus",
"opsworks-cm:describeServers",
"opsworks:describeAgentVersions",
"opsworks:describeApps",
"opsworks:describeCommands",
"opsworks:describeDeployments",
"opsworks:describeEcsClusters",
```

```
"opsworks:describeElasticIps",
"opsworks:describeElasticLoadBalancers",
"opsworks:describeInstances",
"opsworks:describeLayers",
"opsworks:describeLoadBasedAutoScaling",
"opsworks:describeMyUserProfile",
"opsworks:describePermissions",
"opsworks:describeRaidArrays",
"opsworks:describeRdsDbInstances",
"opsworks:describeServiceErrors",
"opsworks:describeStackProvisioningParameters",
"opsworks:describeStacks",
"opsworks:describeStackSummary",
"opsworks:describeTimeBasedAutoScaling",
"opsworks:describeUserProfiles",
"opsworks:describeVolumes",
"opsworks:getHostnameSuggestion",
"organizations:listAccounts",
"organizations:listTagsForResource",
"outposts:getCatalogItem",
"outposts:getConnection",
"outposts:getOrder",
"outposts:getOutpost",
"outposts:getOutpostInstanceTypes",
"outposts:getSite",
"outposts:listAssets",
"outposts:listCatalogItems",
"outposts:listOrders",
"outposts:listOutposts",
"outposts:listSites",
"personalize:describeAlgorithm",
"personalize:describeBatchInferenceJob",
"personalize:describeBatchSegmentJob",
"personalize:describeCampaign",
"personalize:describeDataset",
"personalize:describeDatasetExportJob",
"personalize:describeDatasetGroup",
"personalize:describeDatasetImportJob",
"personalize:describeEventTracker",
"personalize:describeFeatureTransformation",
"personalize:describeFilter",
"personalize:describeRecipe",
"personalize:describeRecommender",
"personalize:describeSchema",
```

```
"personalize:describeSolution",
"personalize:describeSolutionVersion",
"personalize:getPersonalizedRanking",
"personalize:getRecommendations",
"personalize:getSolutionMetrics",
"personalize:listBatchInferenceJobs",
"personalize:listBatchSegmentJobs",
"personalize:listCampaigns",
"personalize:listDatasetExportJobs",
"personalize:listDatasetGroups",
"personalize:listDatasetImportJobs",
"personalize:listDatasets",
"personalize:listEventTrackers",
"personalize:listRecipes",
"personalize:listRecommenders",
"personalize:listSchemas",
"personalize:listSolutions",
"personalize:listSolutionVersions",
"pipes:describePipe",
"pipes:listPipes",
"pipes:listTagsForResource",
"polly:describeVoices",
"polly:getLexicon",
"polly:listLexicons",
"pricing:describeServices",
"pricing:getAttributeValues",
"pricing:getProducts",
"private-networks:getDeviceIdentifier",
"private-networks:getNetwork",
"private-networks:getNetworkResource",
"private-networks:listDeviceIdentifiers",
"private-networks:listNetworks",
"private-networks:listNetworkResources",
"quicksight:describeAccountCustomization",
"quicksight:describeAccountSettings",
"quicksight:describeAccountSubscription",
"quicksight:describeAnalysis",
"quicksight:describeAnalysisPermissions",
"quicksight:describeDashboard",
"quicksight:describeDashboardPermissions",
"quicksight:describeDataSet",
"quicksight:describeDataSetPermissions",
"quicksight:describeDataSetRefreshProperties",
"quicksight:describeDataSource",
```

```
"quicksight:describeDataSourcePermissions",
"quicksight:describeFolder",
"quicksight:describeFolderPermissions",
"quicksight:describeFolderResolvedPermissions",
"quicksight:describeGroup",
"quicksight:describeGroupMembership",
"quicksight:describeIAMPolicyAssignment",
"quicksight:describeIngestion",
"quicksight:describeIpRestriction",
"quicksight:describeNamespace",
"quicksight:describeRefreshSchedule",
"quicksight:describeTemplate",
"quicksight:describeTemplateAlias",
"quicksight:describeTemplatePermissions",
"quicksight:describeTheme",
"quicksight:describeThemeAlias",
"quicksight:describeThemePermissions",
"quicksight:describeTopic",
"quicksight:describeTopicPermissions",
"quicksight:describeTopicRefresh",
"quicksight:describeTopicRefreshSchedule",
"quicksight:describeUser",
"quicksight:describeVPCConnection",
"quicksight:listAnalyses",
"quicksight:listDashboards",
"quicksight:listDashboardVersions",
"quicksight:listDataSets",
"quicksight:listDataSources",
"quicksight:listFolderMembers",
"quicksight:listFolders",
"quicksight:listGroupMemberships",
"quicksight:listGroups",
"quicksight:listIAMPolicyAssignments",
"quicksight:listIAMPolicyAssignmentsForUser",
"quicksight:listIngestions",
"quicksight:listNamespaces",
"quicksight:listRefreshSchedules",
"quicksight:listTemplateAliases",
"quicksight:listTemplates",
"quicksight:listTemplateVersions",
"quicksight:listThemeAliases",
"quicksight:listThemes",
"quicksight:listThemeVersions",
"quicksight:listTopicRefreshSchedules",
```

```
"quicksight:listTopics",
"quicksight:listUserGroups",
"quicksight:listUsers",
"quicksight:listVPCConnections",
"quicksight:searchAnalyses",
"quicksight:searchDashboards",
"quicksight:searchDataSets",
"quicksight:searchDataSources",
"quicksight:searchFolders",
"quicksight:searchGroups",
"ram:getPermission",
"ram:getResourceShareAssociations",
"ram:getResourceShareInvitations",
"ram:getResourceShares",
"ram:listPendingInvitationResources",
"ram:listPrincipals",
"ram:listResources",
"ram:listResourceSharePermissions",
"rbin:getRule",
"rbin:listRules",
"rds:describeAccountAttributes",
"rds:describeBlueGreenDeployments",
"rds:describeCertificates",
"rds:describeDBClusterEndpoints",
"rds:describeDBClusterParameterGroups",
"rds:describeDBClusterParameters",
"rds:describeDBClusters",
"rds:describeDBClusterSnapshots",
"rds:describeDBEngineVersions",
"rds:describeDBInstanceAutomatedBackups",
"rds:describeDBInstances",
"rds:describeDBLogFiles",
"rds:describeDBParameterGroups",
"rds:describeDBParameters",
"rds:describeDBSecurityGroups",
"rds:describeDBSnapshotAttributes",
"rds:describeDBSnapshots",
"rds:describeDBSubnetGroups",
"rds:describeEngineDefaultClusterParameters",
"rds:describeEngineDefaultParameters",
"rds:describeEventCategories",
"rds:describeEvents",
"rds:describeEventSubscriptions",
"rds:describeExportTasks",
```

```
"rds:describeGlobalClusters",
"rds:describeIntegrations",
"rds:describeOptionGroupOptions",
"rds:describeOptionGroups",
"rds:describeOrderableDBInstanceOptions",
"rds:describePendingMaintenanceActions",
"rds:describeReservedDBInstances",
"rds:describeReservedDBInstancesOfferings",
"rds:describeSourceRegions",
"rds:describeValidDBInstanceModifications",
"rds:listTagsForResource",
"redshift-data:describeStatement",
"redshift-data:listStatements",
"redshift:describeClusterParameterGroups",
"redshift:describeClusterParameters",
"redshift:describeClusters",
"redshift:describeClusterSecurityGroups",
"redshift:describeClusterSnapshots",
"redshift:describeClusterSubnetGroups",
"redshift:describeClusterVersions",
"redshift:describeDataShares",
"redshift:describeDataSharesForConsumer",
"redshift:describeDataSharesForProducer",
"redshift:describeDefaultClusterParameters",
"redshift:describeEventCategories",
"redshift:describeEvents",
"redshift:describeEventSubscriptions",
"redshift:describeHsmClientCertificates",
"redshift:describeHsmConfigurations",
"redshift:describeLoggingStatus",
"redshift:describeOrderableClusterOptions",
"redshift:describeReservedNodeOfferings",
"redshift:describeReservedNodes",
"redshift:describeResize",
"redshift:describeSnapshotCopyGrants",
"redshift:describeStorage",
"redshift:describeTableRestoreStatus",
"redshift:describeTags",
"redshift-serverless:getEndpointAccess",
"redshift-serverless:getNamespace",
"redshift-serverless:getRecoveryPoint",
"redshift-serverless:getSnapshot",
"redshift-serverless:getTableRestoreStatus",
"redshift-serverless:getUsageLimit",
```

```
"redshift-serverless:getWorkgroup",
"redshift-serverless:listEndpointAccess",
"redshift-serverless:listNamespaces",
"redshift-serverless:listRecoveryPoints",
"redshift-serverless:listSnapshots",
"redshift-serverless:listTableRestoreStatus",
"redshift-serverless:listUsageLimits",
"redshift-serverless:listWorkgroups",
"rekognition:listCollections",
"rekognition:listFaces",
"resource-explorer-2:getAccountLevelServiceConfiguration",
"resource-explorer-2:getIndex",
"resource-explorer-2:getView",
"resource-explorer-2:listIndexes",
"resource-explorer-2:listViews",
"resource-explorer-2:search",
"resource-groups:getGroup",
"resource-groups:getGroupQuery",
"resource-groups:getTags",
"resource-groups:listGroupResources",
"resource-groups:listGroups",
"resource-groups:searchResources",
"robomaker:batchDescribeSimulationJob",
"robomaker:describeDeploymentJob",
"robomaker:describeFleet",
"robomaker:describeRobot",
"robomaker:describeRobotApplication",
"robomaker:describeSimulationApplication",
"robomaker:describeSimulationJob",
"robomaker:listDeploymentJobs",
"robomaker:listFleets",
"robomaker:listRobotApplications",
"robomaker:listRobots",
"robomaker:listSimulationApplications",
"robomaker:listSimulationJobs",
"route53-recovery-cluster:getRoutingControlState",
"route53-recovery-cluster:listRoutingControls",
"route53-recovery-control-config:describeControlPanel",
"route53-recovery-control-config:describeRoutingControl",
"route53-recovery-control-config:describeSafetyRule",
"route53-recovery-control-config:listControlPanels",
"route53-recovery-control-config:listRoutingControls",
"route53-recovery-control-config:listSafetyRules",
"route53-recovery-readiness:getCell",
```

```
"route53-recovery-readiness:getCellReadinessSummary",
"route53-recovery-readiness:getReadinessCheck",
"route53-recovery-readiness:getReadinessCheckResourceStatus",
"route53-recovery-readiness:getReadinessCheckStatus",
"route53-recovery-readiness:getRecoveryGroup",
"route53-recovery-readiness:getRecoveryGroupReadinessSummary",
"route53-recovery-readiness:listCells",
"route53-recovery-readiness:listReadinessChecks",
"route53-recovery-readiness:listRecoveryGroups",
"route53-recovery-readiness:listResourceSets",
"route53:getAccountLimit",
"route53:getChange",
"route53:getCheckerIpRanges",
"route53:getDNSSEC",
"route53:getGeoLocation",
"route53:getHealthCheck",
"route53:getHealthCheckCount",
"route53:getHealthCheckLastFailureReason",
"route53:getHealthCheckStatus",
"route53:getHostedZone",
"route53:getHostedZoneCount",
"route53:getHostedZoneLimit",
"route53:getQueryLoggingConfig",
"route53:getReusableDelegationSet",
"route53:getTrafficPolicy",
"route53:getTrafficPolicyInstance",
"route53:getTrafficPolicyInstanceCount",
"route53:listCidrBlocks",
"route53:listCidrCollections",
"route53:listCidrLocations",
"route53:listGeoLocations",
"route53:listHealthChecks",
"route53:listHostedZones",
"route53:listHostedZonesByName",
"route53:listHostedZonesByVpc",
"route53:listQueryLoggingConfigs",
"route53:listResourceRecordSets",
"route53:listReusableDelegationSets",
"route53:listTrafficPolicies",
"route53:listTrafficPolicyInstances",
"route53:listTrafficPolicyInstancesByHostedZone",
"route53:listTrafficPolicyInstancesByPolicy",
"route53:listTrafficPolicyVersions",
"route53:listVPCAssociationAuthorizations",
```



```
"route53domains:checkDomainAvailability",
"route53domains:getContactReachabilityStatus",
"route53domains:getDomainDetail",
"route53domains:getOperationDetail",
"route53domains:listDomains",
"route53domains:listOperations",
"route53domains:listPrices",
"route53domains:listTagsForDomain",
"route53domains:viewBilling",
"route53resolver:getFirewallConfig",
"route53resolver:getFirewallDomainList",
"route53resolver:getFirewallRuleGroup",
"route53resolver:getFirewallRuleGroupAssociation",
"route53resolver:getFirewallRuleGroupPolicy",
"route53resolver:getOutpostResolver",
"route53resolver:getResolverDnssecConfig",
"route53resolver:getResolverQueryLogConfig",
"route53resolver:getResolverQueryLogConfigAssociation",
"route53resolver:getResolverQueryLogConfigPolicy",
"route53resolver:getResolverRule",
"route53resolver:getResolverRuleAssociation",
"route53resolver:getResolverRulePolicy",
"route53resolver:listFirewallConfigs",
"route53resolver:listFirewallDomainLists",
"route53resolver:listFirewallDomains",
"route53resolver:listFirewallRuleGroupAssociations",
"route53resolver:listFirewallRuleGroups",
"route53resolver:listFirewallRules",
"route53resolver:listOutpostResolvers",
"route53resolver:listResolverConfigs",
"route53resolver:listResolverDnssecConfigs",
"route53resolver:listResolverEndpointIpAddresses",
"route53resolver:listResolverEndpoints",
"route53resolver:listResolverQueryLogConfigAssociations",
"route53resolver:listResolverQueryLogConfigs",
"route53resolver:listResolverRuleAssociations",
"route53resolver:listResolverRules",
"route53resolver:listTagsForResource",
"rum:batchGetRumMetricDefinitions",
"rum:getAppMonitor",
"rum:listAppMonitors",
"rum:listRumMetricsDestinations",
"s3:describeJob",
"s3:describeMultiRegionAccessPointOperation",
```

```
"s3:getAccelerateConfiguration",
"s3:getAccessPoint",
"s3:getAccessPointConfigurationForObjectLambda",
"s3:getAccessPointForObjectLambda",
"s3:getAccessPointPolicy",
"s3:getAccessPointPolicyForObjectLambda",
"s3:getAccessPointPolicyStatus",
"s3:getAccessPointPolicyStatusForObjectLambda",
"s3:getAccountPublicAccessBlock",
"s3:getAnalyticsConfiguration",
"s3:getBucketAcl",
"s3:getBucketCORS",
"s3:getBucketLocation",
"s3:getBucketLogging",
"s3:getBucketNotification",
"s3:getBucketObjectLockConfiguration",
"s3:getBucketOwnershipControls",
"s3:getBucketPolicy",
"s3:getBucketPolicyStatus",
"s3:getBucketPublicAccessBlock",
"s3:getBucketRequestPayment",
"s3:getBucketVersioning",
"s3:getBucketWebsite",
"s3:getEncryptionConfiguration",
"s3:getIntelligentTieringConfiguration",
"s3:getInventoryConfiguration",
"s3:getLifecycleConfiguration",
"s3:getMetricsConfiguration",
"s3:getMultiRegionAccessPoint",
"s3:getMultiRegionAccessPointPolicy",
"s3:getMultiRegionAccessPointPolicyStatus",
"s3:getMultiRegionAccessPointRoutes",
"s3:getObjectLegalHold",
"s3:getObjectRetention",
"s3:getReplicationConfiguration",
"s3:getStorageLensConfiguration",
"s3:listAccessPoints",
"s3:listAccessPointsForObjectLambda",
"s3:listAllMyBuckets",
"s3:listBucket",
"s3:listBucketMultipartUploads",
"s3:listBucketVersions",
"s3:listJobs",
"s3:listMultipartUploadParts",
```

```
"s3:listMultiRegionAccessPoints",
"s3:listStorageLensConfigurations",
"s3express:listAllMyDirectoryBuckets",
"sagemaker:describeAction",
"sagemaker:describeAlgorithm",
"sagemaker:describeApp",
"sagemaker:describeAppImageConfig",
"sagemaker:describeArtifact",
"sagemaker:describeAutoMLJob",
"sagemaker:describeCodeRepository",
"sagemaker:describeCompilationJob",
"sagemaker:describeContext",
"sagemaker:describeDataQualityJobDefinition",
"sagemaker:describeDevice",
"sagemaker:describeDeviceFleet",
"sagemaker:describeDomain",
"sagemaker:describeEdgeDeploymentPlan",
"sagemaker:describeEdgePackagingJob",
"sagemaker:describeEndpoint",
"sagemaker:describeEndpointConfig",
"sagemaker:describeExperiment",
"sagemaker:describeFeatureGroup",
"sagemaker:describeFeatureMetadata",
"sagemaker:describeFlowDefinition",
"sagemaker:describeHub",
"sagemaker:describeHubContent",
"sagemaker:describeHumanTaskUi",
"sagemaker:describeHyperParameterTuningJob",
"sagemaker:describeImage",
"sagemaker:describeImageVersion",
"sagemaker:describeInferenceExperiment",
"sagemaker:describeInferenceRecommendationsJob",
"sagemaker:describeLabelingJob",
"sagemaker:describeModel",
"sagemaker:describeModelBiasJobDefinition",
"sagemaker:describeModelCard",
"sagemaker:describeModelCardExportJob",
"sagemaker:describeModelExplainabilityJobDefinition",
"sagemaker:describeModelPackage",
"sagemaker:describeModelPackageGroup",
"sagemaker:describeModelQualityJobDefinition",
"sagemaker:describeMonitoringSchedule",
"sagemaker:describeNotebookInstance",
"sagemaker:describeNotebookInstanceLifecycleConfig",
```

```
"sagemaker:describePipeline",
"sagemaker:describePipelineDefinitionForExecution",
"sagemaker:describePipelineExecution",
"sagemaker:describeProcessingJob",
"sagemaker:describeProject",
"sagemaker:describeSpace",
"sagemaker:describeStudioLifecycleConfig",
"sagemaker:describeSubscribedWorkteam",
"sagemaker:describeTrainingJob",
"sagemaker:describeTransformJob",
"sagemaker:describeTrial",
"sagemaker:describeTrialComponent",
"sagemaker:describeUserProfile",
"sagemaker:describeWorkforce",
"sagemaker:describeWorkteam",
"sagemaker:getDeviceFleetReport",
"sagemaker:getModelPackageGroupPolicy",
"sagemaker:getSagemakerServicecatalogPortfolioStatus",
"sagemaker:listActions",
"sagemaker:listAlgorithms",
"sagemaker:listAliases",
"sagemaker:listAppImageConfigs",
"sagemaker:listApps",
"sagemaker:listArtifacts",
"sagemaker:listAssociations",
"sagemaker:listAutoMLJobs",
"sagemaker:listCandidatesForAutoMLJob",
"sagemaker:listCodeRepositories",
"sagemaker:listCompilationJobs",
"sagemaker:listContexts",
"sagemaker:listDataQualityJobDefinitions",
"sagemaker:listDeviceFleets",
"sagemaker:listDevices",
"sagemaker:listDomains",
"sagemaker:listEdgeDeploymentPlans",
"sagemaker:listEdgePackagingJobs",
"sagemaker:listEndpointConfigs",
"sagemaker:listEndpoints",
"sagemaker:listExperiments",
"sagemaker:listFeatureGroups",
"sagemaker:listFlowDefinitions",
"sagemaker:listHubContents",
"sagemaker:listHubContentVersions",
"sagemaker:listHubs",
```

```
"sagemaker:listHumanTaskUis",
"sagemaker:listHyperParameterTuningJobs",
"sagemaker:listImages",
"sagemaker:listImageVersions",
"sagemaker:listInferenceExperiments",
"sagemaker:listInferenceRecommendationsJobs",
"sagemaker:listInferenceRecommendationsJobSteps",
"sagemaker:listLabelingJobs",
"sagemaker:listLabelingJobsForWorkteam",
"sagemaker:listLineageGroups",
"sagemaker:listModelBiasJobDefinitions",
"sagemaker:listModelCardExportJobs",
"sagemaker:listModelCards",
"sagemaker:listModelCardVersions",
"sagemaker:listModelExplainabilityJobDefinitions",
"sagemaker:listModelMetadata",
"sagemaker:listModelPackageGroups",
"sagemaker:listModelPackages",
"sagemaker:listModelQualityJobDefinitions",
"sagemaker:listModels",
"sagemaker:listMonitoringAlertHistory",
"sagemaker:listMonitoringAlerts",
"sagemaker:listMonitoringExecutions",
"sagemaker:listMonitoringSchedules",
"sagemaker:listNotebookInstanceLifecycleConfigs",
"sagemaker:listNotebookInstances",
"sagemaker:listPipelineExecutions",
"sagemaker:listPipelineExecutionSteps",
"sagemaker:listPipelineParametersForExecution",
"sagemaker:listPipelines",
"sagemaker:listProcessingJobs",
"sagemaker:listProjects",
"sagemaker:listSpaces",
"sagemaker:listStageDevices",
"sagemaker:listStudioLifecycleConfigs",
"sagemaker:listSubscribedWorkteams",
"sagemaker:listTags",
"sagemaker:listTrainingJobs",
"sagemaker:listTrainingJobsForHyperParameterTuningJob",
"sagemaker:listTransformJobs",
"sagemaker:listTrialComponents",
"sagemaker:listTrials",
"sagemaker:listUserProfiles",
"sagemaker:listWorkforces",
```

```
"sagemaker:listWorkteams",
"savingsplans:describeSavingsPlans",
"scheduler:getSchedule",
"scheduler:getScheduleGroup",
"scheduler:listScheduleGroups",
"scheduler:listSchedules",
"schemas:describeCodeBinding",
"schemas:describeDiscoverer",
"schemas:describeRegistry",
"schemas:describeSchema",
"schemas:getCodeBindingSource",
"schemas:getDiscoveredSchema",
"schemas:getResourcePolicy",
"schemas:listDiscoverers",
"schemas:listRegistries",
"schemas:listSchemas",
"schemas:listSchemaVersions",
"sdb:domainMetadata",
"sdb:listDomains",
"secretsmanager:describeSecret",
"secretsmanager:getResourcePolicy",
"secretsmanager:listSecrets",
"secretsmanager:listSecretVersionIds",
"securityhub:getEnabledStandards",
"securityhub:getFindings",
"securityhub:getInsightResults",
"securityhub:getInsights",
"securityhub:getMasterAccount",
"securityhub:getMembers",
"securityhub:listEnabledProductsForImport",
"securityhub:listInvitations",
"securityhub:listMembers",
"securitylake:getDataLakeExceptionSubscription",
"securitylake:getDataLakeOrganizationConfiguration",
"securitylake:getDataLakeSources",
"securitylake:getSubscriber",
"securitylake:listDataLakeExceptions",
"securitylake:listDataLakes",
"securitylake:listLogSources",
"securitylake:listSubscribers",
"serverlessrepo:getApplication",
"serverlessrepo:getApplicationPolicy",
"serverlessrepo:getCloudFormationTemplate",
"serverlessrepo:listApplicationDependencies",
```

```
"serverlessrepo:listApplications",
"serverlessrepo:listApplicationVersions",
"servicecatalog:describeConstraint",
"servicecatalog:describePortfolio",
"servicecatalog:describeProduct",
"servicecatalog:describeProductAsAdmin",
"servicecatalog:describeProductView",
"servicecatalog:describeProvisioningArtifact",
"servicecatalog:describeProvisioningParameters",
"servicecatalog:describeRecord",
"servicecatalog:listAcceptedPortfolioShares",
"servicecatalog:listConstraintsForPortfolio",
"servicecatalog:listLaunchPaths",
"servicecatalog:listPortfolioAccess",
"servicecatalog:listPortfolios",
"servicecatalog:listPortfoliosForProduct",
"servicecatalog:listPrincipalsForPortfolio",
"servicecatalog:listProvisioningArtifacts",
"servicecatalog:listRecordHistory",
"servicecatalog:scanProvisionedProducts",
"servicecatalog:searchProducts",
"servicequotas:getAssociationForServiceQuotaTemplate",
"servicequotas:getAWSDefaultServiceQuota",
"servicequotas:getRequestedServiceQuotaChange",
"servicequotas:getServiceQuota",
"servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:listAWSDefaultServiceQuotas",
"servicequotas:listRequestedServiceQuotaChangeHistory",
"servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:listServiceQuotas",
"servicequotas:listServices",
"ses:describeActiveReceiptRuleSet",
"ses:describeConfigurationSet",
"ses:describeReceiptRule",
"ses:describeReceiptRuleSet",
"ses:getAccount",
"ses:getAccountSendingEnabled",
"ses:getBlacklistReports",
"ses:getConfigurationSet",
"ses:getConfigurationSetEventDestinations",
"ses:getContactList",
"ses:getDedicatedIp",
"ses:getDedicatedIpPool",
```

```
"ses:getDedicatedIps",
"ses:getDeliverabilityDashboardOptions",
"ses:getDeliverabilityTestReport",
"ses:getDomainDeliverabilityCampaign",
"ses:getDomainStatisticsReport",
"ses:getEmailIdentity",
"ses:getIdentityDkimAttributes",
"ses:getIdentityMailFromDomainAttributes",
"ses:getIdentityNotificationAttributes",
"ses:getIdentityPolicies",
"ses:getIdentityVerificationAttributes",
"ses:getImportJob",
"ses:getSendQuota",
"ses:getSendStatistics",
"ses:listConfigurationSets",
"ses:listContactLists",
"ses:listContacts",
"ses:listCustomVerificationEmailTemplates",
"ses:listDedicatedIpPools",
"ses:listDeliverabilityTestReports",
"ses:listDomainDeliverabilityCampaigns",
"ses:listEmailIdentities",
"ses:listEmailTemplates",
"ses:listIdentities",
"ses:listIdentityPolicies",
"ses:listImportJobs",
"ses:listReceiptFilters",
"ses:listReceiptRuleSets",
"ses:listRecommendations",
"ses:listTagsForResource",
"ses:listTemplates",
"ses:listVerifiedEmailAddresses",
"shield:describeAttack",
"shield:describeProtection",
"shield:describeSubscription",
"shield:listAttacks",
"shield:listProtections",
"sms-voice:getConfigurationSetEventDestinations",
"sms:getConnectors",
"sms:getReplicationJobs",
"sms:getReplicationRuns",
"sms:getServers",
"snowball:describeAddress",
"snowball:describeAddresses",
```



```
"snowball:describeJob",
"snowball:getSnowballUsage",
"snowball:listJobs",
"snowball:listServiceVersions",
"sns:checkIfPhoneNumberIsOptedOut",
"sns:getDataProtectionPolicy",
"sns:getEndpointAttributes",
"sns:getPlatformApplicationAttributes",
"sns:getSMSAttributes",
"sns:getSMSSandboxAccountStatus",
"sns:getSubscriptionAttributes",
"sns:getTopicAttributes",
"sns:listEndpointsByPlatformApplication",
"sns:listOriginationNumbers",
"sns:listPhoneNumbersOptedOut",
"sns:listPlatformApplications",
"sns:listSMSSandboxPhoneNumbers",
"sns:listSubscriptions",
"sns:listSubscriptionsByTopic",
"sns:listTopics",
"sqs:getQueueAttributes",
"sqs:getQueueUrl",
"sqs:listDeadLetterSourceQueues",
"sqs:listQueues",
"ssm-contacts:describeEngagement",
"ssm-contacts:describePage",
"ssm-contacts:getContact",
"ssm-contacts:getContactChannel",
"ssm-contacts:getContactPolicy",
"ssm-contacts:getRotation",
"ssm-contacts:getRotationOverride",
"ssm-contacts:listContactChannels",
"ssm-contacts:listContacts",
"ssm-contacts:listEngagements",
"ssm-contacts:listPageReceipts",
"ssm-contacts:listPageResolutions",
"ssm-contacts:listPagesByContact",
"ssm-contacts:listPagesByEngagement",
"ssm-contacts:listPreviewRotationShifts",
"ssm-contacts:listRotationOverrides",
"ssm-contacts:listRotations",
"ssm-contacts:listRotationShifts",
"ssm-incidents:getIncidentRecord",
"ssm-incidents:getReplicationSet",
```

```
"ssm-incidents:getResourcePolicies",
"ssm-incidents:getResponsePlan",
"ssm-incidents:getTimelineEvent",
"ssm-incidents:listIncidentRecords",
"ssm-incidents:listRelatedItems",
"ssm-incidents:listReplicationSets",
"ssm-incidents:listResponsePlans",
"ssm-incidents:listTimelineEvents",
"ssm-sap:getApplication",
"ssm-sap:getComponent",
"ssm-sap:getDatabase",
"ssm-sap:getOperation",
"ssm-sap:getResourcePermission",
"ssm-sap:listApplications",
"ssm-sap:listComponents",
"ssm-sap:listDatabases",
"ssm-sap:listOperations",
"ssm:describeActivations",
"ssm:describeAssociation",
"ssm:describeAssociationExecutions",
"ssm:describeAssociationExecutionTargets",
"ssm:describeAutomationExecutions",
"ssm:describeAutomationStepExecutions",
"ssm:describeAvailablePatches",
"ssm:describeDocument",
"ssm:describeDocumentPermission",
"ssm:describeEffectiveInstanceAssociations",
"ssm:describeEffectivePatchesForPatchBaseline",
"ssm:describeInstanceAssociationsStatus",
"ssm:describeInstanceInformation",
"ssm:describeInstancePatches",
"ssm:describeInstancePatchStates",
"ssm:describeInstancePatchStatesForPatchGroup",
"ssm:describeInventoryDeletions",
"ssm:describeMaintenanceWindowExecutions",
"ssm:describeMaintenanceWindowExecutionTaskInvocations",
"ssm:describeMaintenanceWindowExecutionTasks",
"ssm:describeMaintenanceWindows",
"ssm:describeMaintenanceWindowSchedule",
"ssm:describeMaintenanceWindowsForTarget",
"ssm:describeMaintenanceWindowTargets",
"ssm:describeMaintenanceWindowTasks",
"ssm:describeOpsItems",
"ssm:describeParameters",
```

```
"ssm:describePatchBaselines",
"ssm:describePatchGroups",
"ssm:describePatchGroupState",
"ssm:describePatchProperties",
"ssm:describeSessions",
"ssm:getAutomationExecution",
"ssm:getCalendarState",
"ssm:getCommandInvocation",
"ssm:getConnectionStatus",
"ssm:getDefaultPatchBaseline",
"ssm:getDeployablePatchSnapshotForInstance",
"ssm:getInventorySchema",
"ssm:getMaintenanceWindow",
"ssm:getMaintenanceWindowExecution",
"ssm:getMaintenanceWindowExecutionTask",
"ssm:getMaintenanceWindowExecutionTaskInvocation",
"ssm:getMaintenanceWindowTask",
"ssm:getOpsItem",
"ssm:getOpsMetadata",
"ssm:getOpsSummary",
"ssm:getPatchBaseline",
"ssm:getPatchBaselineForPatchGroup",
"ssm:getResourcePolicies",
"ssm:getServiceSetting",
"ssm:listAssociations",
"ssm:listAssociationVersions",
"ssm:listCommandInvocations",
"ssm:listCommands",
"ssm:listComplianceItems",
"ssm:listComplianceSummaries",
"ssm:listDocuments",
"ssm:listDocumentMetadataHistory",
"ssm:listDocumentVersions",
"ssm:listOpsItemEvents",
"ssm:listOpsItemRelatedItems",
"ssm:listOpsMetadata",
"ssm:listResourceComplianceSummaries",
"ssm:listResourceDataSync",
"ssm:listTagsForResource",
"sso:describeApplicationAssignment",
"sso:describeApplicationProvider",
"sso:describeApplication",
"sso:describeInstance",
"sso:describeTrustedTokenIssuer",
```

```
"sso:getApplicationAccessScope",
"sso:getApplicationAssignmentConfiguration",
"sso:getApplicationAuthenticationMethod",
"sso:getApplicationGrant",
"sso:getApplicationInstance",
"sso:getApplicationTemplate",
"sso:getManagedApplicationInstance",
"sso:getSharedSsoConfiguration",
"sso:listApplicationAccessScopes",
"sso:listApplicationAssignments",
"sso:listApplicationAuthenticationMethods",
"sso:listApplicationGrants",
"sso:listApplicationInstances",
"sso:listApplicationProviders",
"sso:listApplications",
"sso:listApplicationTemplates",
"sso:listDirectoryAssociations",
"sso:listInstances",
"sso:listProfileAssociations",
"sso:listTrustedTokenIssuers",
"states:describeActivity",
"states:describeExecution",
"states:describeMapRun",
"states:describeStateMachine",
"states:describeStateMachineAlias",
"states:describeStateMachineForExecution",
"states:getExecutionHistory",
"states:listActivities",
"states:listExecutions",
"states:listMapRuns",
"states:listStateMachineAliases",
"states:listStateMachines",
"states:listStateMachineVersions",
"storagegateway:describeBandwidthRateLimit",
"storagegateway:describeCache",
"storagegateway:describeCachediSCSIVolumes",
"storagegateway:describeFileSystemAssociations",
"storagegateway:describeGatewayInformation",
"storagegateway:describeMaintenanceStartTime",
"storagegateway:describeNFSFileShares",
"storagegateway:describeSMBFileShares",
"storagegateway:describeSMBSettings",
"storagegateway:describeSnapshotSchedule",
"storagegateway:describeStorediSCSIVolumes",
```

```
"storagegateway:describeTapeArchives",
"storagegateway:describeTapeRecoveryPoints",
"storagegateway:describeTapes",
"storagegateway:describeUploadBuffer",
"storagegateway:describeVTLDevices",
"storagegateway:describeWorkingStorage",
"storagegateway:listAutomaticTapeCreationPolicies",
"storagegateway:listFileShares",
"storagegateway:listFileSystemAssociations",
"storagegateway:listGateways",
"storagegateway:listLocalDisks",
"storagegateway:listTagsForResource",
"storagegateway:listTapes",
"storagegateway:listVolumeInitiators",
"storagegateway:listVolumeRecoveryPoints",
"storagegateway:listVolumes",
"swf:countClosedWorkflowExecutions",
"swf:countOpenWorkflowExecutions",
"swf:countPendingActivityTasks",
"swf:countPendingDecisionTasks",
"swf:describeActivityType",
"swf:describeDomain",
"swf:describeWorkflowExecution",
"swf:describeWorkflowType",
"swf:getWorkflowExecutionHistory",
"swf:listActivityTypes",
"swf:listClosedWorkflowExecutions",
"swf:listDomains",
"swf:listOpenWorkflowExecutions",
"swf:listWorkflowTypes",
"synthetics:describeCanaries",
"synthetics:describeCanariesLastRun",
"synthetics:describeRuntimeVersions",
"synthetics:getCanary",
"synthetics:getCanaryRuns",
"synthetics:getGroup",
"synthetics:listAssociatedGroups",
"synthetics:listGroupResources",
"synthetics:listGroups",
"tiros:createQuery",
"tiros:getQueryAnswer",
"tiros:getQueryExplanation",
"transcribe:describeLanguageModel",
"transcribe:getCallAnalyticsCategory",
```

```
"transcribe:getCallAnalyticsJob",
"transcribe:getMedicalTranscriptionJob",
"transcribe:getMedicalVocabulary",
"transcribe:getTranscriptionJob",
"transcribe:getVocabulary",
"transcribe:getVocabularyFilter",
"transcribe:listCallAnalyticsCategories",
"transcribe:listCallAnalyticsJobs",
"transcribe:listLanguageModels",
"transcribe:listMedicalTranscriptionJobs",
"transcribe:listMedicalVocabularies",
"transcribe:listTranscriptionJobs",
"transcribe:listVocabularies",
"transcribe:listVocabularyFilters",
"transfer:describeAccess",
"transfer:describeAgreement",
"transfer:describeConnector",
"transfer:describeExecution",
"transfer:describeProfile",
"transfer:describeServer",
"transfer:describeUser",
"transfer:describeWorkflow",
"transfer:listAccesses",
"transfer:listAgreements",
"transfer:listConnectors",
"transfer:listExecutions",
"transfer:listHostKeys",
"transfer:listProfiles",
"transfer:listServers",
"transfer:listTagsForResource",
"transfer:listUsers",
"transfer:listWorkflows",
"transfer:sendWorkflowStepState",
"trustedadvisor:getOrganizationRecommendation",
"trustedadvisor:getRecommendation",
"trustedadvisor:listChecks",
"trustedadvisor:listOrganizationRecommendationAccounts",
"trustedadvisor:listOrganizationRecommendationResources",
"trustedadvisor:listOrganizationRecommendations",
"trustedadvisor:listRecommendationResources",
"trustedadvisor:listRecommendations",
"verifiedpermissions:getIdentitySource",
"verifiedpermissions:getPolicy",
"verifiedpermissions:getPolicyStore",
```

```
"verifiedpermissions:getPolicyTemplate",
"verifiedpermissions:getSchema",
"verifiedpermissions:listIdentitySources",
"verifiedpermissions:listPolicies",
"verifiedpermissions:listPolicyStores",
"verifiedpermissions:listPolicyTemplates",
"vpc-lattice:getAccessLogSubscription",
"vpc-lattice:getAuthPolicy",
"vpc-lattice:getListener",
"vpc-lattice:getResourcePolicy",
"vpc-lattice:getRule",
"vpc-lattice:getService",
"vpc-lattice:getServiceNetwork",
"vpc-lattice:getServiceNetworkServiceAssociation",
"vpc-lattice:getServiceNetworkVpcAssociation",
"vpc-lattice:getTargetGroup",
"vpc-lattice:listAccessLogSubscriptions",
"vpc-lattice:listListeners",
"vpc-lattice:listRules",
"vpc-lattice:listServiceNetworks",
"vpc-lattice:listServiceNetworkServiceAssociations",
"vpc-lattice:listServiceNetworkVpcAssociations",
"vpc-lattice:listServices",
"vpc-lattice:listTargetGroups",
"vpc-lattice:listTargets",
"waf-regional:getByteMatchSet",
"waf-regional:getChangeTokenStatus",
"waf-regional:getGeoMatchSet",
"waf-regional:getIPSet",
"waf-regional:getLoggingConfiguration",
"waf-regional:getRateBasedRule",
"waf-regional:getRegexMatchSet",
"waf-regional:getRegexPatternSet",
"waf-regional:getRule",
"waf-regional:getRuleGroup",
"waf-regional:getSqlInjectionMatchSet",
"waf-regional:getWebACL",
"waf-regional:getWebACLForResource",
"waf-regional:listActivatedRulesInRuleGroup",
"waf-regional:listByteMatchSets",
"waf-regional:listGeoMatchSets",
"waf-regional:listIPSets",
"waf-regional:listLoggingConfigurations",
"waf-regional:listRateBasedRules",
```

```
"waf-regional:listRegexMatchSets",
"waf-regional:listRegexPatternSets",
"waf-regional:listResourcesForWebACL",
"waf-regional:listRuleGroups",
"waf-regional:listRules",
"waf-regional:listSqlInjectionMatchSets",
"waf-regional:listWebACLs",
"waf:getByteMatchSet",
"waf:getChangeTokenStatus",
"waf:getGeoMatchSet",
"waf:getIPSet",
"waf:getLoggingConfiguration",
"waf:getRateBasedRule",
"waf:getRegexMatchSet",
"waf:getRegexPatternSet",
"waf:getRule",
"waf:getRuleGroup",
"waf:getSampledRequests",
"waf:getSizeConstraintSet",
"waf:getSqlInjectionMatchSet",
"waf:getWebACL",
"waf:getXssMatchSet",
"waf:listActivatedRulesInRuleGroup",
"waf:listByteMatchSets",
"waf:listGeoMatchSets",
"waf:listIPSets",
"waf:listLoggingConfigurations",
"waf:listRateBasedRules",
"waf:listRegexMatchSets",
"waf:listRegexPatternSets",
"waf:listRuleGroups",
"waf:listRules",
"waf:listSizeConstraintSets",
"waf:listSqlInjectionMatchSets",
"waf:listWebACLs",
"waf:listXssMatchSets",
"wafv2:checkCapacity",
"wafv2:describeManagedRuleGroup",
"wafv2:getIPSet",
"wafv2:getLoggingConfiguration",
"wafv2:getPermissionPolicy",
"wafv2:getRateBasedStatementManagedKeys",
"wafv2:getRegexPatternSet",
"wafv2:getRuleGroup",
```



```
"wafv2:getSampledRequests",
"wafv2:getWebACL",
"wafv2:getWebACLForResource",
"wafv2:listAvailableManagedRuleGroups",
"wafv2:listIPSets",
"wafv2:listLoggingConfigurations",
"wafv2:listRegexPatternSets",
"wafv2:listResourcesForWebACL",
"wafv2:listRuleGroups",
"wafv2:listTagsForResource",
"wafv2:listWebACLs",
"workdocs:checkAlias",
"workdocs:describeAvailableDirectories",
"workdocs:describeInstances",
"workmail:describeGroup",
"workmail:describeOrganization",
"workmail:describeResource",
"workmail:describeUser",
"workmail:listAliases",
"workmail:listGroupMembers",
"workmail:listGroups",
"workmail:listMailboxPermissions",
"workmail:listOrganizations",
"workmail:listResourceDelegates",
"workmail:listResources",
"workmail:listUsers",
"workspaces-web:getBrowserSettings",
"workspaces-web:getIdentityProvider",
"workspaces-web:getNetworkSettings",
"workspaces-web:getPortal",
"workspaces-web:getPortalServiceProviderMetadata",
"workspaces-web:getTrustStoreCertificate",
"workspaces-web:getUserSettings",
"workspaces-web:listBrowserSettings",
"workspaces-web:listIdentityProviders",
"workspaces-web:listNetworkSettings",
"workspaces-web:listPortals",
"workspaces-web:listTagsForResource",
"workspaces-web:listTrustStoreCertificates",
"workspaces-web:listTrustStores",
"workspaces-web:listUserSettings",
"workspaces:describeAccount",
"workspaces:describeAccountModifications",
"workspaces:describeIpGroups",
```

```
    "workspaces:describeTags",
    "workspaces:describeWorkspaceBundles",
    "workspaces:describeWorkspaceDirectories",
    "workspaces:describeWorkspaceImages",
    "workspaces:describeWorkspaces",
    "workspaces:describeWorkspacesConnectionStatus"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
}
],
"Version" : "2012-10-17"
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

AWSSystemsManagerAccountDiscoveryServicePolicy est une [politique AWS gérée](#) qui : autorise AWS Systems Manager (SSM) à découvrir le compte AWS des informations.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 24 octobre 2019, 17:21 UTC
- Heure modifiée : 17 octobre 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy est une [politique AWS gérée](#) qui : fournit un accès aux AWS ressources gérées ou utilisées par le framework de gestion des modifications de AWS Systems Manager.

Utilisation des politiques politiques politiques politiques politiques

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les groupes.

Les détails politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 7 décembre 2020, 22:21 UTC
- Heure modifiée : 7 décembre 2020, 22h21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui permet à d'effectuer les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON de stratégie

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


Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSystemsManagerForSAPReadOnlyAccess

AWSSystemsManagerForSAPReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule au service AWS Systems Manager for SAP

Utilisation de cette stratégie

Vous pouvez les associer AWSSystemsManagerForSAPReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 17 novembre 2022, 02:11 UTC
- Heure modifiée : 17 novembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
        "ssm-sap:get*",
        "ssm-sap:list*"
    ],
    "Resource" : "arn:*:ssm-sap:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

AWSSystemsManagerOpsDataSyncServiceRolePolicy est une [politique AWS gérée](#) qui : rôle IAM pour SSM Explorer pour gérer les opérations connexes OpsData

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 26 avril 2021, 20:42 UTC
- Heure modifiée : 28 juin 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
```

```
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "securityhub:GetFindings",
    "securityhub:BatchUpdateFindings"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Confidence" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Criticality" : false
    }
  }
},
},
```

```
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Note.Text" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/RelatedFindings" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Types" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
```

```
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy est une [politique AWS gérée](#) qui : Cette politique accorde au AWS Portal Asset Server les autorisations nécessaires à son fonctionnement normal.

Utilisation de cette stratégie

Vous pouvez `AWSThinkboxAssetServerPolicy` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:18 UTC
- Heure modifiée : 27 mai 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:PutObject",
        "s3:ListBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxAWSPortalAdminPolicy

AWSThinkboxAWSPortalAdminPolicy est une [politique AWS gérée](#) qui : Cette politique accorde au logiciel Deadline de AWS Thinkbox un accès complet à plusieurs AWS services requis pour l'administration AWS du portail. Cela inclut l'accès pour créer des balises arbitraires sur plusieurs types de ressources EC2.

Utilisation de cette politique

Vous pouvez vous associer AWSThinkboxAWSPortalAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:41 UTC
- Heure modifiée : 23 février 2024, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
```



```
    "ec2:DescribeNatGateways",
    "ec2:DescribeTags",
    "ec2:DescribeKeyPairs",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeRegions",
    "ec2:DescribeSpotFleetRequestHistory",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotFleetInstances",
    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:GetConsoleOutput",
    "ec2:ImportKeyPair",
    "ec2:ReleaseAddress",
    "ec2:RequestSpotFleet",
    "ec2:CancelSpotFleetRequests",
    "ec2:DisassociateAddress",
    "ec2>DeleteFleets",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteVpc",
    "ec2>DeletePlacementGroup",
    "ec2>DeleteVpcEndpoints",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2:DisassociateRouteTable",
    "ec2>DeleteSubnet",
    "ec2>DeleteNatGateway",
    "ec2:DetachInternetGateway",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifyFleet",
    "ec2:ModifySpotFleetRequest",
    "ec2:ModifyVpcAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal2",
  "Effect" : "Allow",
```

```

    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:key-pair/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:launch-template/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:placement-group/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:image/*"
    ]
  },
  {
    "Sid" : "AWSThinkboxAWSPortal3",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:InstanceProfile" : "arn:aws:iam:*:*:instance-profile/AWSPortal*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal4",
    "Effect" : "Allow",
    "Action" : "ec2:TerminateInstances",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal5",
    "Effect" : "Allow",
    "Action" : "ec2:TerminateInstances",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
      }
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal6",
    "Effect" : "Allow",
    "Action" : "ec2:TerminateInstances",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal7",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
```

```
    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:internet-gateway/*",
    "arn:aws:ec2:*:*:route-table/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:natgateway/*",
    "arn:aws:ec2:*:*:elastic-ip/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal10",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal11",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:instance-profile/AWSPortal*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal12",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetPolicy",
    "iam:ListEntitiesForPolicy",
    "iam:ListPolicyVersions"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:policy/AWSPortal*"
  ]
},
{
```

```
"Sid" : "AWSThinkboxAWSPortal13",
"Effect" : "Allow",
"Action" : [
  "iam:GetRole",
  "iam:GetRolePolicy"
],
"Resource" : [
  "arn:aws:iam::*:role/AWSPortal*",
  "arn:aws:iam::*:role/DeadlineSpot*"
]
},
{
  "Sid" : "AWSThinkboxAWSPortal14",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal15",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com"
      ]
    }
  }
}
```

```

    ]
  }
}
},
{
  "Sid" : "AWSThinkboxAWSPortal16",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:PutBucketAcl",
    "s3:PutBucketCORS",
    "s3:PutBucketVersioning",
    "s3:GetBucketAcl",
    "s3:GetObject",
    "s3:PutBucketLogging",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3>DeleteBucketPolicy",
    "s3>DeleteObjectVersion"
  ],
  "Resource" : [
    "arn:aws:s3::*:awsportal*",
    "arn:aws:s3::*:stack*",
    "arn:aws:s3::*:aws-portal-cache*",
    "arn:aws:s3::*:logs-for-aws-portal-cache*",
    "arn:aws:s3::*:logs-for-stack*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal17",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy"
  ],
  "Resource" : [

```

```
    "arn:aws:s3::*:logs-for-aws-portal-cache*"
  ],
},
{
  "Sid" : "AWSThinkboxAWSPortal18",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketOwnershipControls"
  ],
  "Resource" : [
    "arn:aws:s3::*:logs-for-stack*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal19",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal20",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:Scan"
  ],
  "Resource" : "arn:aws:dynamodb::*:table/DeadlineFleetHealth*"
},
{
  "Sid" : "AWSThinkboxAWSPortal21",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation>DeleteStack",
    "cloudformation>DeleteChangeSet",
    "cloudformation:ListStackResources",
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:UpdateTerminationProtection"
  ],
},
```

```
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/stack*/**",
      "arn:aws:cloudformation:*:*:stack/Deadline*/**"
    ]
  },
  {
    "Sid" : "AWSThinkboxAWSPortal22",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:EstimateTemplateCost",
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSThinkboxAWSPortal23",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents",
      "logs:PutRetentionPolicy",
      "logs>DeleteRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
  },
  {
    "Sid" : "AWSThinkboxAWSPortal24",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups",
      "logs:CreateLogGroup"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSThinkboxAWSPortal25",
    "Effect" : "Allow",
    "Action" : [
      "kms:Encrypt",
      "kms:GenerateDataKey"
    ],
    "Resource" : [
      "*"
    ]
  }
}
```



```
    ],
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "s3.*.amazonaws.com",
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal26",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:Name" : [
          "rcs-tls-pw*"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal27",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DeleteSecret",
      "secretsmanager:UpdateSecret",
      "secretsmanager:DescribeSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy est une [politique AWS gérée](#) qui : Cette politique accorde à la machine AWS Portal Gateway les autorisations nécessaires à son fonctionnement normal.

Utilisation de cette stratégie

Vous pouvez AWSThinkboxAWSPortalGatewayPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:05 UTC
- Heure modifiée : 30 juin 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "logs:DescribeLogGroups",
    "logs:CreateLogStream"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-portal-cache*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "dynamodb:Scan",
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*"
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*/gateway_certs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:rds-tls-pw-stack*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxAWSPortalWorkerPolicy

AWSThinkboxAWSPortalWorkerPolicy est une [politique AWS gérée](#) qui : Cette politique accorde aux Deadline Workers de AWS Portal les autorisations nécessaires à un fonctionnement normal.

Utilisation de cette stratégie

Vous pouvez AWSThinkboxAWSPortalWorkerPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mai 2020, 19:15 UTC
- Heure modifiée : 7 décembre 2020, 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-portal-cache*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*/gateway_certs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:SendMessage",
    "sqs:GetQueueUrl"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWS*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

AWSThinkboxDeadlineResourceTrackerAccessPolicy est une [politiqueAWS gérée](#) qui : accorde les autorisations requises pour le fonctionnement du Deadline Resource Tracker deAWS Thinkbox. Cela inclut un accès complet à certaines actions EC2, notamment DeleteFleets et CancelSpotFleetRequests.

Utilisation de cette stratégie

Vous pouvez les associerAWSThinkboxDeadlineResourceTrackerAccessPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mai 2020, 19:25 UTC
- Heure modifiée : 27 mai 2020, 19:25 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb>DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",

```



```

    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CancelSpotFleetRequests",
    "ec2>DeleteFleets",
    "ec2:DescribeFleetInstances",
    "ec2:DescribeFleets",
    "ec2:DescribeInstances",
    "ec2:DescribeSpotFleetInstances",
    "ec2:DescribeSpotFleetRequests"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RebootInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutEvents"
  ],
  "Resource" : [
    "arn:aws:events:*:*:event-bus/default"
  ]
},
{

```

```
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:DeleteMessage",
      "sqs:GetQueueAttributes",
      "sqs:ReceiveMessage"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicyest une [politiqueAWS gérée](#) qui : accorde les autorisations requises pour créer, détruire et administrer le Deadline Resource Tracker deAWS Thinkbox.

Utilisation de cette stratégie

Vous pouvezAWSThinkboxDeadlineResourceTrackerAdminPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mai 2020, 19:29 UTC
- Heure modifiée : 22 juin 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DeregisterScalableTarget",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:RegisterScalableTarget"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:UpdateStack",
      "cloudformation:DescribeStacks",
      "cloudformation:UpdateTerminationProtection"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb>CreateTable",
      "dynamodb>DeleteTable",
      "dynamodb:DescribeTable",
```

```
    "dynamodb:ListTagsOfResource",
    "dynamodb:TagResource",
    "dynamodb:UntagResource"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchWriteItem",
    "dynamodb:Scan"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/DeadlineResourceTracker*"
  ]
},
{
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:GetUser"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "dynamodb.application-autoscaling.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "application-autoscaling.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:GetEventSourceMapping"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateEventSourceMapping",
      "lambda>DeleteEventSourceMapping"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "lambda:FunctionArn" : [
          "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission",
      "lambda:RemovePermission"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ],
    "Condition" : {
      "StringLike" : {
        "lambda:Principal" : "events.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda>DeleteFunctionConcurrency",
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration",
      "lambda:ListTags",
      "lambda:PutFunctionConcurrency",
      "lambda:TagResource",
      "lambda:UntagResource",
      "lambda:UpdateFunctionCode",
      "lambda:UpdateFunctionConfiguration"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:/deadline_aws_resource_tracker-*.zip",
      "arn:aws:s3::*:/DeadlineAWSResourceTrackerTemplate-*.yaml"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs>DeleteQueue",
```



```
    "sqs:GetQueueAttributes",
    "sqs:ListQueueTags",
    "sqs:TagQueue",
    "sqs:UntagQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
    "arn:aws:sqs:*:*:DeadlineResourceTracker*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

AWSThinkboxDeadlineSpotEventPluginAdminPolicyest une [politiqueAWS gérée](#) qui : accorde les autorisations requises pour le plugin Deadline Spot Event deAWS Thinkbox. Cela inclut l'autorisation de demander, de modifier et d'annuler une flotte ponctuelle, ainsi que PassRole l'autorisation limitée.

Utilisation de cette stratégie

Vous pouvezAWSThinkboxDeadlineSpotEventPluginAdminPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mai 2020, 19:38 UTC
- Heure modifiée : 27 mai 2020, 19:38 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam::*:instance-profile/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicyest une [politiqueAWS gérée](#) qui : accorde les autorisations requises pour une instance EC2 exécutant le logicielAWS Thinkbox Deadline Spot Event Plugin Worker.

Utilisation de cette stratégie

Vous pouvez les associerAWSThinkboxDeadlineSpotEventPluginWorkerPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 mai 2020, 19:35 UTC
- Heure modifiée : 7 décembre 2020, 23h31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeTags"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueUrl",
```

```
    "sqs:SendMessage"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTransferConsoleFullAccess

AWSTransferConsoleFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet àAWS Transfer via leAWS Management Console

Utilisation de cette stratégie

Vous pouvezAWSTransferConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 décembre 2020, 19:33 UTC
- Heure modifiée : 14 décembre 2020, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTransferFullAccess

AWSTransferFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet au service deAWS transfert.

Utilisation de cette stratégie

Vous pouvezAWSTransferFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 décembre 2020, 19:37 UTC
- Heure modifiée : 14 décembre 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "transfer:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "transfer.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeAddresses"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTransferLoggingAccess

AWSTransferLoggingAccess est une [politique AWS gérée](#) qui : Permet de AWS transférer un accès complet pour créer des flux de journaux et des groupes et enregistrer les événements sur votre compte

Utilisation de cette stratégie

Vous pouvez les associer `AWSTransferLoggingAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 janvier 2019, 15:32 UTC
- Heure modifiée : 14 janvier 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTransferReadOnlyAccess

AWSTransferReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule aux servicesAWS de transfert.

Utilisation de cette stratégie

Vous pouvezAWSTransferReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 août 2020, 17:54 UTC
- Heure modifiée : 27 août 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Effect" : "Allow",
"Action" : [
  "transfer:DescribeUser",
  "transfer:DescribeServer",
  "transfer:ListUsers",
  "transfer:ListServers",
  "transfer:TestIdentityProvider",
  "transfer:ListTagsForResource"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AWS Trusted Advisor Priority. Cette politique permet également à l'utilisateur d'ajouter comme service de confiance avec AWS Organizations et de spécifier les comptes administrateurs délégués pour Trusted Advisor Priority.

Utilisation de cette politique

Vous pouvez AWSTrustedAdvisorPriorityFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 16 août 2022, 16:08 UTC
- Heure modifiée : 16 août 2022, 16:08 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor>DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "reporting.trustedadvisor.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "arn:aws:organizations::*:*:*:*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "reporting.trustedadvisor.amazonaws.com"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers vers vers les autorisations de moindre privilège](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule àAWS Trusted Advisor Priority. Cela inclut l'autorisation de consulter les comptes d'administrateur délégué.

Utilisation de cette stratégie

Vous pouvezAWSTrustedAdvisorPriorityReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 16 août 2022, 16:35 UTC
- Heure modifiée : 16 août 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "trustedadvisor:DescribeAccount*",
      "trustedadvisor:DescribeOrganization",
      "trustedadvisor:DescribeRisk*",
      "trustedadvisor:DownloadRisk",
      "trustedadvisor:DescribeNotificationConfigurations"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "reporting.trustedadvisor.amazonaws.com"
        ]
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy est une [politiqueAWS gérée qui](#) : Politique de service pour les rapports multicomptes de Trusted Advisor

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 novembre 2019, 17:41 UTC
- Heure modifiée : 28 février 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListChildren",
    "organizations:ListParents",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy est une [politique AWS gérée](#) qui : Accédez au service AWS Trusted Advisor pour vous aider à réduire les coûts, à augmenter les performances et à améliorer la sécurité de votre AWS environnement.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 22 février 2018, 21:24 UTC
- Heure modifiée : 18 janvier 2024, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
```

```
"ec2:DescribeSubnets",
"ec2:DescribeRegions",
"ec2:DescribeReservedInstancesOfferings",
"ec2:DescribeSnapshots",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DescribeLaunchTemplateVersions",
"ecs:DescribeTaskDefinition",
"ecs:ListTaskDefinitions",
"elasticloadbalancing:DescribeAccountLimits",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetServerCertificate",
"iam:ListServerCertificates",
"kinesis:DescribeLimits",
"kafka:ListClustersV2",
"kafka:ListNodes",
"outposts:ListAssets",
"outposts:GetOutpost",
"outposts:ListOutposts",
"rds:DescribeAccountAttributes",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEvents",
"rds:DescribeOptionGroupOptions",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribeReservedDBInstances",
"rds:DescribeReservedDBInstancesOfferings",
```

```

    "rds:ListTagsForResource",
    "redshift:DescribeClusters",
    "redshift:DescribeReservedNodeOfferings",
    "redshift:DescribeReservedNodes",
    "route53:GetAccountLimit",
    "route53:GetHealthCheck",
    "route53:GetHostedZone",
    "route53:ListHealthChecks",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets",
    "route53resolver:ListResolverEndpoints",
    "route53resolver:ListResolverEndpointIpAddresses",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetLifecycleConfiguration",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "ses:GetSendQuota",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : autorise les notifications AWS utilisateur à appeler AWS des services en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, vos groupes ou vos rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 19 avril 2023, 13:28 UTC
- Heure modifiée : 19 avril 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events>DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/Notifications"
      }
    },
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à la consultation des ressources Vendor Insights et à la gestion des abonnements Vendor Insights

Utilisation de cette stratégie

Vous pouvez AWSVendorInsightsAssessorFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 1 décembre 2022, 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "artifact:GetReport",
  "artifact:GetReportMetadata",
  "artifact:GetTermForReport",
  "artifact:ListReports"
],
"Resource" : "arn:aws:artifact:*::report/*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnlyest une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule pour consulter les ressources Vendor Insights autorisées

Utilisation de cette stratégie

Vous pouvezAWSVendorInsightsAssessorReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 01 décembre 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSVendorInsightsVendorFullAccess

AWSVendorInsightsVendorFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à la création et à la gestion des ressources Vendor Insights

Utilisation de cette politique

Vous pouvez vous associer AWSVendorInsightsVendorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 19 octobre 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "vendor-insights:CreateDataSource",
    "vendor-insights:UpdateDataSource",
    "vendor-insights>DeleteDataSource",
    "vendor-insights:GetDataSource",
    "vendor-insights:ListDataSources",
    "vendor-insights:CreateSecurityProfile",
    "vendor-insights:ListSecurityProfiles",
    "vendor-insights:GetSecurityProfile",
    "vendor-insights:AssociateDataSource",
    "vendor-insights:DisassociateDataSource",
    "vendor-insights:UpdateSecurityProfile",
    "vendor-insights:ActivateSecurityProfile",
    "vendor-insights:DeactivateSecurityProfile",
    "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
    "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
    "vendor-insights:ListSecurityProfileSnapshots",
    "vendor-insights:GetSecurityProfileSnapshot",
    "vendor-insights:TagResource",
    "vendor-insights:UntagResource",
    "vendor-insights:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:AcceptAgreementApprovalRequest",
    "aws-marketplace:RejectAgreementApprovalRequest",
    "aws-marketplace:GetAgreementApprovalRequest",
    "aws-marketplace:ListAgreementApprovalRequests",
    "aws-marketplace:CancelAgreement",
    "aws-marketplace:SearchAgreements"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
    }
  }
},
{

```

```
"Effect" : "Allow",
"Action" : [
  "artifact:GetReport",
  "artifact:GetReportMetadata",
  "artifact:GetTermForReport",
  "artifact:ListReports"
],
"Resource" : "arn:aws:artifact:*::report/*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule pour consulter les ressources Vendor Insights

Utilisation de cette stratégie

Vous pouvez AWSVendorInsightsVendorReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 1 décembre 2022, 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/*SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "arn:aws:artifact:*::report/*"  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSVpcLatticeServiceRolePolicy

AWSVpcLatticeServiceRolePolicyest une [politiqueAWS gérée](#) qui : Autorise VPC Lattice à accéder auxAWS ressources en votre nom.

Utilisation des stratégies politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les des politique politique politique

- Type : Politique de rôles liée à un service
- Heure de création : 30 novembre 2022
- Heure modifiée : 30 novembre 2022, 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 6 août 2019, 14:13 UTC
- Heure modifiée : 6 août 2019, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSVPCTransitGatewayServiceRolePolicy

AWSVPCTransitGatewayServiceRolePolicy est une [politique AWS gérée](#) qui : autorise VPC Transit Gateway à créer et à gérer les ressources nécessaires pour vos pièces jointes VPC Transit Gateway.

Utilisation utilisation utilisation utilisation utilisation utilisation utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les groupes.

Les détails politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 26 novembre 2018, 16:21 UTC
- Heure modifiée : 15 avril 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

politique Jpolitique Jpolitique Jpolitique

```
{
  "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"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques gérées gérées et évoluez les politiquesAWS gérées gérées de moindre privilège gérées et évoluez les autorisations de moindre privilège gérées](#)

AWSVPCVerifiedAccessServiceRolePolicy

AWSVPCVerifiedAccessServiceRolePolicyest une [politique AWS gérée](#) qui : Politique permettant au service AWS Verified Access de fournir des terminaux en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 29 novembre 2022, 03:35 UTC
- Heure modifiée : 17 novembre 2023, 21h03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
    "arn:aws:ec2:*:*:security-group/*"
  ],
},
{
  "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/VerifiedAccessManaged" : "true"
    }
  }
},
{
  "Sid" : "VerifiedAccessRoleTaggingActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    }
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSWAFConsoleFullAccess

AWSWAFConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à AWS WAF via le AWS Management Console. Notez que cette politique accorde également l'autorisation

de répertorier et de mettre à jour les CloudFront distributions Amazon, l'autorisation de consulter les équilibreurs de charge sur AWS Elastic Load Balancing, l'autorisation de consulter les API et les étapes REST d'Amazon API Gateway, l'autorisation de répertorier et de consulter CloudWatch les métriques Amazon, et l'autorisation d'afficher les régions activées au sein du compte.

Utilisation de cette stratégie

Vous pouvez l'associer `AWSWAFConsoleFullAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 avril 2020, 18:38 UTC
- Heure modifiée : 5 juin 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:SetWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:GetMetricData",

```

```

    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:DescribeRegions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:SetWebACL",
    "appsync:ListGraphQLApis",
    "appsync:SetWebACL",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "s3:ListAllMyBuckets",
    "logs:DescribeResourcePolicies",
    "logs:DescribeLogGroups",
    "cognito-idp:ListUserPools",
    "cognito-idp:AssociateWebACL",
    "cognito-idp:DisassociateWebACL",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-idp:GetWebACLForResource",
    "apprunner:AssociateWebAcl",
    "apprunner:DisassociateWebAcl",
    "apprunner:DescribeWebAclForService",
    "apprunner:ListServices",
    "apprunner:ListAssociatedServicesForWebAcl",
    "ec2:AssociateVerifiedAccessInstanceWebAcl",
    "ec2:DisassociateVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
    "ec2:GetVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowLogDeliverySubscription",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs>DeleteLogDelivery"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
  "Action" : [
    "s3:PutBucketPolicy",

```



```
    "s3:GetBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-waf-logs-*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
  "Action" : [
    "logs:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Effect" : "Allow",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "wafv2.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWAFConsoleReadOnlyAccess

AWSWAFConsoleReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à AWS WAF via le. AWS Management Console Notez que cette politique accorde également l'autorisation de répertorier les CloudFront distributions Amazon, l'autorisation de consulter les équilibrateurs de charge sur AWS Elastic Load Balancing, l'autorisation de consulter les API et les étapes REST d'Amazon API Gateway, l'autorisation de répertorier et de consulter CloudWatch les métriques Amazon, ainsi que l'autorisation d'afficher les régions activées au sein du compte.

Utilisation de cette stratégie

Vous pouvez l'associer `AWSWAFConsoleReadOnlyAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 avril 2020, 18:43 UTC
- Heure modifiée : 5 juin 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "apigateway:GET",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "appsync:ListGraphQLApis",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
      ]
    }
  ]
}
```

```
    "wafv2:Describe*",
    "wafv2:Get*",
    "wafv2:List*",
    "wafv2:CheckCapacity",
    "cognito-idp:ListUserPools",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-idp:GetWebACLForResource",
    "apprunner:DescribeWebAclForService",
    "apprunner:ListServices",
    "apprunner:ListAssociatedServicesForWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
    "ec2:GetVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstances"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWAFFullAccess

AWSWAFFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux actions AWS WAF.

Utilisation de cette stratégie

Vous pouvez l'associer AWSWAFFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 octobre 2015, 20:44 UTC

- Heure modifiée : 5 juin 2023, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*",
        "wafv2:*",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "appsync:SetWebACL",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "AllowLogDeliverySubscription",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs>DeleteLogDelivery"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutBucketPolicy",
      "s3:GetBucketPolicy"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-waf-logs-*"
    ]
  },
  {
    "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutResourcePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "wafv2.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarez avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWAFReadOnlyAccess

AWSWAFReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux actions AWS WAF.

Utilisation de cette stratégie

Vous pouvez AWSWAFReadOnlyAccess l'associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 octobre 2015, 20:43 UTC
- Heure modifiée : 5 juin 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
```

```
    "waf-regional:List*",
    "wafv2:Get*",
    "wafv2:List*",
    "wafv2:Describe*",
    "wafv2:CheckCapacity",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-idp:GetWebACLForResource",
    "apprunner:DescribeWebAclForService",
    "apprunner:ListServices",
    "apprunner:ListAssociatedServicesForWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
    "ec2:GetVerifiedAccessInstanceWebAcl"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrez avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy est une [politique AWS gérée](#) qui : Permet d'accéder WellArchitected aux AWS services et aux ressources liés aux WellArchitected ressources pour le compte des clients.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 26 avril 2023, 18:36 UTC
- Heure modifiée : 26 avril 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicecatalog:*:*/applications/*",
    "arn:*:servicecatalog:*:*/attribute-groups/AWS_WellArchitected-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog>DeleteAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicecatalog:*:*/attribute-groups/AWS_WellArchitected-*"
  ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

AWSWellArchitectedOrganizationsServiceRolePolicy est une [politique AWS gérée](#) qui :
Autorise Well-Architected à accéder aux Organizations en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 juin 2022, 17:15 UTC
- Heure modifiée : 25 juillet 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",

```

```
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSWickrFullAccess

AWSWickrFullAccess est une [politiqueAWS gérée](#) qui : Cette politique accorde des autorisations administratives complètes au service Wickr, y compris les fonctions administratives de Wickr dans le cadre duAWS Management Console.

Utilisation de cette stratégie

Vous pouvez les associerAWSWickrFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2022, 20:36 UTC
- Heure modifiée : 27 novembre 2022, 20:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSXrayCrossAccountSharingConfiguration

AWSXrayCrossAccountSharingConfiguration est une [politiqueAWS gérée](#) qui : fournit des fonctionnalités permettant de gérer les liens d'Observability Access Manager et d'établir le partage des traces X-Ray

Utilisation de cette stratégie

Vous pouvez AWSXrayCrossAccountSharingConfiguration les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2022, 13:46 UTC
- Heure modifiée : 27 novembre 2022, 13:46 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSXRayDaemonWriteAccess

AWSXRayDaemonWriteAccess est une [politique AWS gérée](#) qui : autorise le AWS X-Ray Daemon à relayer les données brutes des segments de trace vers l'API du service et à récupérer les données d'échantillonnage (règles, cibles, etc.) à utiliser par le SDK X-Ray.

Utilisation de cette politique

Vous pouvez vous associer AWSXRayDaemonWriteAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 août 2018, 23h00 UTC
- Heure modifiée : 13 février 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSXrayFullAccess

AWSXrayFullAccess est une [politique AWS gérée qui : Politique gérée](#) d'accès complet à AWS X-Ray

Utilisation de cette stratégie

Vous pouvez AWSXrayFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 1 décembre 2016, 18h30 UTC
- Heure modifiée : 01 décembre 2016, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSXrayReadOnlyAccess

AWSXrayReadOnlyAccess est une [politique AWS gérée qui : politique gérée](#) en lecture seule de AWS X-Ray

Utilisation de cette politique

Vous pouvez vous associer AWSXrayReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 18:27 UTC
- Heure modifiée : 14 février 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
```

```
    "xray:GetServiceGraph",
    "xray:GetTraceGraph",
    "xray:GetTraceSummaries",
    "xray:GetGroups",
    "xray:GetGroup",
    "xray:ListTagsForResource",
    "xray:ListResourcePolicies",
    "xray:GetTimeSeriesServiceStatistics",
    "xray:GetInsightSummaries",
    "xray:GetInsight",
    "xray:GetInsightEvents",
    "xray:GetInsightImpactGraph"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

AWSXrayWriteOnlyAccess

AWSXrayWriteOnlyAccess est une [politique AWS gérée](#) qui :AWS X-Ray écrit uniquement une politique gérée

Utilisation de cette stratégie

Vous pouvez AWSXrayWriteOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée

- Heure de création : 1 décembre 2016, 18:19 UTC
- Heure modifiée : 28 août 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

AWSZonalAutoshiftPracticeRunSLRPolicy est une [politique AWS gérée](#) qui : fournit un accès administratif pour les essais par changement de zone ARC et un accès aux états des CloudWatch alarmes pour surveiller les essais.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 29 novembre 2023, 17:34 UTC
- Heure modifiée : 29 novembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ZonalShiftManagementPermissions",
    "Effect" : "Allow",
    "Action" : [
      "arc-zonal-shift:CancelZonalShift",
      "arc-zonal-shift:GetManagedResource",
      "arc-zonal-shift:StartZonalShift",
      "arc-zonal-shift:UpdateZonalShift"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

BatchServiceRolePolicy

BatchServiceRolePolicy est une [politique AWS gérée](#) qui : fournit un accès au service AWS Batch pour gérer les ressources requises, y compris les ressources Amazon EC2 et Amazon ECS.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 10 mars 2021, 06:55 UTC
- Heure modifiée : 5 décembre 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
```

```

    "ecs:DescribeTasks",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "ecs:ListTasks",
    "ecs:DeregisterTaskDefinition",
    "ecs:TagResource",
    "ecs:ListAccountSettings",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
},
{
  "Sid" : "AWSBatchPolicyStatement3",
  "Effect" : "Allow",
  "Action" : [
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
},
{
  "Sid" : "AWSBatchPolicyStatement4",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:CreateOrUpdateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
}

```

```
  },
  {
    "Sid" : "AWSBatchPolicyStatement5",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn",
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement6",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com",
          "autoscaling.amazonaws.com",
          "ecs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement7",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSBatchServiceTag" : "false"
      }
    }
  }
}
```



```

    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CancelSpotFleetRequests",
      "ec2:ModifySpotFleetRequest",
      "ec2>DeleteLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSBatchServiceTag" : "false"
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement9",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteLaunchConfiguration"
    ],
    "Resource" :
"arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement10",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:SetDesiredCapacity",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling:SuspendProcesses",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:TerminateInstanceInAutoScalingGroup"
    ],
    "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
  },

```

```
{
  "Sid" : "AWSBatchPolicyStatement11",
  "Effect" : "Allow",
  "Action" : [
    "ecs:DeleteCluster",
    "ecs:DeregisterContainerInstance",
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
},
{
  "Sid" : "AWSBatchPolicyStatement12",
  "Effect" : "Allow",
  "Action" : [
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:task-definition/*"
},
{
  "Sid" : "AWSBatchPolicyStatement13",
  "Effect" : "Allow",
  "Action" : [
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "AWSBatchPolicyStatement14",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
},
},
```

```
{
  "Sid" : "AWSBatchPolicyStatement15",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:ec2:*:*:elastic-gpu/*",
    "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
    "arn:aws:resource-groups:*:*:group*"
  ]
},
{
  "Sid" : "AWSBatchPolicyStatement16",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
```

```
        "CreateLaunchTemplate",
        "RequestSpotFleet"
    ]
}
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

Billing

Billing est une [politique AWS gérée](#) qui : accorde des autorisations pour la facturation et la gestion des coûts. Cela inclut la visualisation de l'utilisation du compte ainsi que l'affichage et la modification des budgets et des modes de paiement.

Utilisation de cette politique

Vous pouvez vous associer Billing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions du poste
- Heure de création : 10 novembre 2016, 17:33 UTC
- Heure modifiée : 17 janvier 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:UpdateBillingPreferences",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets>DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce>DeleteCostCategoryDefinition",
        "ce>DeleteNotificationSubscription",
        "ce>DeleteReport",
        "ce:DescribeCostCategoryDefinition",
```

```
"ce:GetCostAndUsage",
"ce:ListCostAllocationTags",
"ce:ListCostCategoryDefinitions",
"ce:ListTagsForResource",
"ce:TagResource",
"ce:UpdateCostAllocationTagsStatus",
"ce:UpdateNotificationSubscription",
"ce:UpdatePreferences",
"ce:UpdateReport",
"ce:UpdateCostCategoryDefinition",
"ce:UntagResource",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cur:DeleteReportDefinition",
"cur:DescribeReportDefinitions",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"cur:ModifyReportDefinition",
"cur:PutClassicReportPreferences",
"cur:PutReportDefinition",
"cur:ValidateReportDestination",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"freetier:PutFreeTierAlertPreference",
" invoicing: GetInvoiceEmailDeliveryPreferences",
" invoicing: GetInvoicePDF",
" invoicing: ListInvoiceSummaries",
" invoicing: PutInvoiceEmailDeliveryPreferences",
" payments: CreatePaymentInstrument",
" payments: DeletePaymentInstrument",
" payments: GetPaymentInstrument",
" payments: GetPaymentStatus",
" payments: ListPaymentPreferences",
" payments: MakePayment",
" payments: UpdatePaymentPreferences",
" pricing: DescribeServices",
" purchase-orders: AddPurchaseOrder",
" purchase-orders: DeletePurchaseOrder",
" purchase-orders: GetPurchaseOrder",
" purchase-orders: ListPurchaseOrderInvoices",
" purchase-orders: ListPurchaseOrders",
" purchase-orders: ListTagsForResource",
" purchase-orders: ModifyPurchaseOrders",
```

```
    "purchase-orders:TagResource",
    "purchase-orders:UntagResource",
    "purchase-orders:UpdatePurchaseOrder",
    "purchase-orders:UpdatePurchaseOrderStatus",
    "purchase-orders:ViewPurchaseOrders",
    "support:CreateCase",
    "support:AddAttachmentsToSet",
    "sustainability:GetCarbonFootprintSummary",
    "tax:BatchPutTaxRegistration",
    "tax:DeleteTaxRegistration",
    "tax:GetExemptions",
    "tax:GetTaxInheritance",
    "tax:GetTaxInterview",
    "tax:GetTaxRegistration",
    "tax:GetTaxRegistrationDocument",
    "tax:ListTaxRegistrations",
    "tax:PutTaxInheritance",
    "tax:PutTaxInterview",
    "tax:PutTaxRegistration",
    "tax:UpdateExemptions"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CertificateManagerServiceRolePolicy

CertificateManagerServiceRolePolicy [stratégie AWS gérée qui : politique](#) de rôle de service Amazon Certificate Manager des rôles de service qui : politique de rôle de service Amazon

Utilisation de cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 25 juin 2020, 17:56 UTC
- Heure modifiée : 25 juin 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations de stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JAM JAM

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


En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège de moindre privilège de moindre privilège de moindre privilège de](#)

ClientVPNServiceConnectionsRolePolicy

ClientVPNServiceConnectionsRolePolicy est une [politique AWS gérée](#) qui : Politique permettant à AWS Client VPN de gérer les connexions de vos points de terminaison Client VPN.

Utilisation de de de de de des

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos groupes ou les groupes ou les groupes ou les groupes ou les groupes ou les rôles attachés à d'autres

Les des des des des

- Type : Politique de rôles liée à un service
- Heure de création : 12 août 2020, 19:48 UTC
- Heure modifiée : 12 août 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de de de de de des

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées](#)

ClientVPNServiceRolePolicy

ClientVPNServiceRolePolicy est une [politiqueAWS gérée](#) qui : Politique permettant àAWS Client VPN de gérer vos points de terminaison Client VPN.

Utilisation de stratégie

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de politique

- Type : Politique de rôles liée à un service
- Heure de création : 10 décembre 2018
- Heure modifiée : 12 août 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy est une [politiqueAWS gérée](#) qui :
Rôle de service pour CloudFormation StackSets (compte principal de l'organisation)

Utilisation à cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les rôles.

Les détails de la politique

- Type : Politique de rôles liée à un service
- Heure de création : 10 décembre 2019, 00:20 UTC
- Heure modifiée : 10 décembre 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut à la stratégie est la version qui définit les autorisations à la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAssumeRoleInMemberAccounts",
    "Effect" : "Allow",
    "Action" : "sts:AssumeRole",
    "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

CloudFormationStackSetsOrgMemberServiceRolePolicy est une [politiqueAWS gérée](#) qui :
Rôle de service pour CloudFormation StackSets (compte membre de l'organisation)

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 9 décembre 2019, 23:52 UTC
- Heure modifiée : 9 décembre 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudFrontFullAccess

CloudFrontFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à la CloudFront console ainsi que la possibilité de répertorier les compartiments Amazon S3 via le AWS Management Console.

Utilisation de cette politique

Vous pouvez vous associer CloudFrontFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 4 janvier 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    }
  ],
}
```

```
{
  "Sid" : "cffullaccess",
  "Action" : [
    "acm:ListCertificates",
    "cloudfront:*",
    "cloudfront-keyvaluestore:*",
    "iam:ListServerCertificates",
    "waf:ListWebACLs",
    "waf:GetWebACL",
    "wafv2:ListWebACLs",
    "wafv2:GetWebACL",
    "kinesis:ListStreams"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "cffdescribestream",
  "Action" : [
    "kinesis:DescribeStream"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:kinesis:*:*:*"
},
{
  "Sid" : "cfflistroles",
  "Action" : [
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudFrontReadOnlyAccess

CloudFrontReadOnlyAccess est une [politique AWS gérée](#) qui : donne accès aux informations de configuration de CloudFront distribution et répertorie les distributions via le AWS Management Console.

Utilisation de cette politique

Vous pouvez vous associer CloudFrontReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 4 janvier 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
      ]
    }
  ]
}
```

```
    "cloudfront-keyvaluestore:Describe*",
    "cloudfront-keyvaluestore:Get*",
    "cloudfront-keyvaluestore:List*",
    "iam:ListServerCertificates",
    "route53:List*",
    "waf:ListWebACLs",
    "waf:GetWebACL",
    "wafv2:ListWebACLs",
    "wafv2:GetWebACL"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudHSMServiceRolePolicy

CloudHSMServiceRolePolicy est une [politique AWS gérée](#) qui : Permet l'accès aux AWS ressources utilisées ou gérées par CloudHSM

Utilisation politiques Utilisation politiques

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails détails politiques

- Type : Politique de rôles liée à un service
- Heure de création : 6 novembre 2017, 19:12 UTC
- Heure modifiée : 6 novembre 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document politiques JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations](#)

CloudSearchFullAccess

CloudSearchFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet au service CloudSearch de configuration Amazon.

Utilisation de cette stratégie

Vous pouvez `CloudSearchFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudSearchReadOnlyAccess

CloudSearchReadOnlyAccess est une [politiqueAWS gérée](#) qui : fournit un accès en lecture seule au service CloudSearch de configuration Amazon.

Utilisation de cette stratégie

Vous pouvez CloudSearchReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudTrailServiceRolePolicy

CloudTrailServiceRolePolicy est une [politique AWS gérée](#) qui : Politique d'autorisation pour CloudTrail ServiceLinkedRole

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 24 octobre 2018, 21:21 UTC
- Heure modifiée : 27 novembre 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
```

```
"Resource" : [
  "arn:*:glue:*:*:catalog",
  "arn:*:glue:*:*:database/aws:cloudtrail",
  "arn:*:glue:*:*:table/aws:cloudtrail/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "DeregisterResourceAccess",
  "Effect" : "Allow",
  "Action" : "lakeformation:DeregisterResource",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatch-CrossAccountAccess

CloudWatch-CrossAccountAccess est une [politique AWS gérée](#) qui : Permet CloudWatch d'assumer CloudWatchCrossAccountSharing des rôles sur des comptes distants pour le compte courant afin d'afficher des données entre comptes et entre régions

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 23 juillet 2019, 09:59 UTC
- Heure modifiée : 23 juillet 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchActionsEC2Access

CloudWatchActionsEC2Access est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux CloudWatch alarmes et aux mesures ainsi qu'aux métadonnées EC2. Permet d'accéder à l'arrêt, à l'arrêt et au redémarrage des instances EC2.

Utilisation de cette stratégie

Vous pouvez CloudWatchActionsEC2Access les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 juillet 2015, 00:00 UTC
- Heure modifiée : 07 juillet 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchAgentAdminPolicy

CloudWatchAgentAdminPolicy est une [politique AWS gérée](#) qui : toutes les autorisations sont requises pour l'utiliser AmazonCloudWatchAgent.

Utilisation de cette politique

Vous pouvez vous associer CloudWatchAgentAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2018, 00:52 UTC
- Heure modifiée : 5 février 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy est une [politique AWS gérée](#) qui : Autorisations requises pour une utilisation AmazonCloudWatchAgent sur les serveurs

Utilisation de cette politique

Vous pouvez vous associer CloudWatchAgentServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2018, 01:06 UTC
- Heure modifiée : 6 février 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",

```

```
    "logs:PutRetentionPolicy",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups",
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetSamplingStatisticSummaries"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWASSMServerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchApplicationInsightsFullAccess

CloudWatchApplicationInsightsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à CloudWatch Application Insights et aux dépendances requises.

Utilisation de cette stratégie

Vous pouvez les associer CloudWatchApplicationInsightsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 novembre 2020, 18:44 UTC
- Heure modifiée : 25 janvier 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
```

```
    "sns:ListTopics",
    "states:ListStateMachines",
    "apigateway:GET",
    "ecs:ListClusters",
    "ecs:DescribeTaskDefinition",
    "ecs:ListServices",
    "ecs:ListTasks",
    "eks:ListClusters",
    "eks:ListNodegroups",
    "fsx:DescribeFileSystems",
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "application-insights.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchApplicationInsightsReadOnlyAccess

CloudWatchApplicationInsightsReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à CloudWatch Application Insights.

Utilisation de cette stratégie

Vous pouvezCloudWatchApplicationInsightsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 novembre 2020, 18:48 UTC
- Heure modifiée : 24 novembre 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

CloudwatchApplicationInsightsServiceLinkedRolePolicyest une [politiqueAWS gérée](#) qui : Cloudwatch Application Insights Service Linked Role Policy

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 1 décembre 2018, 16:22 UTC
- Heure modifiée : 11 mai 2023, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v24 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch>DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudFormation:CreateStack",
    "cloudFormation:UpdateStack",
    "cloudFormation>DeleteStack",
    "cloudFormation:DescribeStackResources"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudFormation:DescribeStacks",
    "cloudFormation>ListStackResources",
    "cloudFormation>ListStacks"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups>ListGroupResources",
    "resource-groups:GetGroupQuery",
    "resource-groups:GetGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "resource-groups:CreateGroup",
  "resource-groups>DeleteGroup"
],
"Resource" : [
  "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DescribeAutoScalingGroups"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm>DeleteParameter",
    "ssm:AddTagsToResource",
    "ssm:RemoveTagsFromResource",
    "ssm:GetParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
```

```

    "ssm:UpdateAssociation",
    "ssm>DeleteAssociation",
    "ssm:DescribeAssociation"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:association/*",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
    "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetOpsItem",
    "ssm:CreateOpsItem",
    "ssm:DescribeOpsItems",
    "ssm:UpdateOpsItem",
    "ssm:DescribeInstanceInformation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:opsitem/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListCommandInvocations",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : [
    "*"
  ]
},

```

```
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
    "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
    "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumeStatus",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeNatGateways"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions",
    "lambda:GetFunctionConfiguration",
    "lambda:ListEventSourceMappings"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "xray:GetServiceGraph",
    "xray:GetTraceSummaries",
    "xray:GetTimeSeriesServiceStatistics",
    "xray:GetTraceGraph"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListTables",
    "dynamodb:DescribeTable",
    "dynamodb:DescribeContributorInsights",
    "dynamodb:DescribeTimeToLive"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets"
  ],
  "Resource" : [
```



```
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "apigateway:GET"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
```

```
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListServices",
    "ecs:ListTasks"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateClusterSettings"
  ],
  "Resource" : [
    "arn:aws:ecs:*:*:cluster/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "eks:DescribeCluster",
    "eks:DescribeFargateProfile",
    "eks:DescribeNodegroup",
    "eks:ListClusters",
    "eks:ListFargateProfiles",
    "eks:ListNodegroups",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:GetSubscriptionAttributes",
    "sns:GetTopicAttributes",
    "sns:GetSMSAttributes",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "sqs:ListQueues"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:DeleteSubscriptionFilter"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:PutSubscriptionFilter"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticfilesystem:DescribeFileSystems"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
```

```
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchApplicationSignalsServiceRolePolicy

CloudWatchApplicationSignalsServiceRolePolicy est une [politique AWS gérée](#) qui : Policy autorise CloudWatch Application Signals à collecter des données de surveillance et de balisage auprès d'autres AWS services pertinents.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 09 novembre 2023, 18:09 UTC
- Heure modifiée : 7 mars 2024, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
  },
  {
    "Sid" : "CWLogsPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery",
      "logs:GetQueryResults"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/apps/signals/*:*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "CWMetricsPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
```

```
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchAutomaticDashboardsAccess

CloudWatchAutomaticDashboardsAccess est une [politique AWS gérée](#) qui : fournit un accès aux applications autres que les CloudWatch API utilisées pour afficher les tableaux de bord CloudWatch automatiques, y compris le contenu d'objets tels que les fonctions Lambda

Utilisation de cette stratégie

Vous pouvez CloudWatchAutomaticDashboardsAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 23 juillet 2019, 10:01 UTC
- Heure modifiée : 20 avril 2021, 13:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
    }
  ],
}
```



```
    "Resource" : "*"
  },
  {
    "Action" : [
      "apigateway:GET"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:apigateway:*::/restapis*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchCrossAccountSharingConfiguration

CloudWatchCrossAccountSharingConfiguration est une [politiqueAWS gérée](#) qui : fournit des fonctionnalités permettant de gérer les liens d'Observability Access Manager et d'établir le partage des CloudWatch ressources

Utilisation de cette stratégie

Vous pouvez CloudWatchCrossAccountSharingConfiguration les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2022, 14:01 UTC
- Heure modifiée : 27 novembre 2022, 14:01 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

```
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchEventsBuiltInTargetExecutionAccess

CloudWatchEventsBuiltInTargetExecutionAccess est une [politiqueAWS gérée](#) qui : autorise les cibles intégrées à Amazon CloudWatch Events à effectuer des actions EC2 en votre nom.

Utilisation de cette stratégie

Vous pouvez CloudWatchEventsBuiltInTargetExecutionAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 janvier 2016, 18:35 UTC
- Heure modifiée : 14 janvier 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchEventsFullAccess

CloudWatchEventsFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon CloudWatch Events.

Utilisation de cette stratégie

Vous pouvez les associer CloudWatchEventsFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 14 janvier 2016, 18:37 UTC
- Heure modifiée : 01 décembre 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "schemas.amazonaws.com"
    }
  }
},
{
  "Sid" : "SecretsManagerAccessForApiDestinations",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:UpdateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:PutSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager::*:secret:events!*"
},
{
  "Sid" : "IAMPassRoleForCloudWatchEvents",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
},
{
  "Sid" : "IAMPassRoleAccessForScheduler",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "scheduler.amazonaws.com"
    }
  }
},
},

```

```
{
  "Sid" : "IAMPassRoleAccessForPipes",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "pipes.amazonaws.com"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchEventsInvocationAccess

CloudWatchEventsInvocationAccess est une [politiqueAWS gérée](#) qui : autorise Amazon CloudWatch Events à relayer des événements vers les fluxAWS Kinesis Streams de votre compte.

Utilisation de cette stratégie

Vous pouvez les associerCloudWatchEventsInvocationAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 14 janvier 2016, 18:36 UTC
- Heure modifiée : 14 janvier 2016, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchEventsReadOnlyAccess

CloudWatchEventsReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon CloudWatch Events.

Utilisation de cette stratégie

Vous pouvez `CloudWatchEventsReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 14 janvier 2016, 18:27 UTC
- Heure modifiée : 01 décembre 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",

```

```
    "events:DescribeReplay",
    "events:ListReplays",
    "events:DescribeConnection",
    "events:ListConnections",
    "events:DescribeApiDestination",
    "events:ListApiDestinations",
    "events:DescribeEndpoint",
    "events:ListEndpoints",
    "schemas:DescribeCodeBinding",
    "schemas:DescribeDiscoverer",
    "schemas:DescribeRegistry",
    "schemas:DescribeSchema",
    "schemas:ExportSchema",
    "schemas:GetCodeBindingSource",
    "schemas:GetDiscoveredSchema",
    "schemas:GetResourcePolicy",
    "schemas:ListDiscoverers",
    "schemas:ListRegistries",
    "schemas:ListSchemas",
    "schemas:ListSchemaVersions",
    "schemas:ListTagsForResource",
    "schemas:SearchSchemas",
    "scheduler:GetSchedule",
    "scheduler:GetScheduleGroup",
    "scheduler:ListSchedules",
    "scheduler:ListScheduleGroups",
    "scheduler:ListTagsForResource",
    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchEventsServiceRolePolicy

CloudWatchEventsServiceRolePolicy est une [politique AWS gérée](#) qui : Permet d'AWS CloudWatch exécuter des actions en votre nom configurées par le biais d'alarmes et d'événements.

Utilisation de cette politique politique politique politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique politique à vos groupes ou les groupes de stratégies de stratégie de stratégie de stratégie de stratégie de stratégie de politique de

Utilisation des politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 novembre 2017, 00:42 UTC
- Heure modifiée : 17 novembre 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations de la stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie stratégie politique Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie de politique de politique

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Utilisation stratégiesAWS gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées stratégies gérées](#)

CloudWatchFullAccess

CloudWatchFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à CloudWatch.

Utilisation de cette stratégie

Vous pouvez CloudWatchFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2022, 13:23 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
    }
  ]
}
```

```
    "Resource" : "arn:aws:oam:*:*:sink/*"  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchFullAccessV2

CloudWatchFullAccessV2 est une [politique AWS gérée](#) qui : fournit un accès complet à CloudWatch.

Utilisation de cette politique

Vous pouvez vous associer CloudWatchFullAccessV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 août 2023, 11:32 UTC
- Heure modifiée : 5 décembre 2023, 19:36 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
```

```
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "events.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "OAMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "oam:ListAttachedLinks"
    ],
    "Resource" : "arn:aws:oam::*:sink/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchInternetMonitorServiceRolePolicy

CloudWatchInternetMonitorServiceRolePolicy est un [AWS politique gérée](#) cela : permet à Internet Monitor d'accéder à EC2, aux espaces de travail et CloudFront ressources et autres services requis en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type: Politique des rôles liés au service
- Heure de création: 27 novembre 2022, 17:46 UTC
- Heure de modification :20 juillet 2023, 04h46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy

Version de la politique

Version de la politique : v2(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès àAWSressource,AWSvérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/InternetMonitor"
      }
    },
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy est une [politique AWS gérée](#) qui : Politique requise pour l'extension Lambda Insights

Utilisation de cette stratégie

Vous pouvez CloudWatchLambdaInsightsExecutionRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 7 octobre 2020, 19:27 UTC

- Heure modifiée : 07 octobre 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchLogsCrossAccountSharingConfiguration

CloudWatchLogsCrossAccountSharingConfiguration est une [politique AWS gérée](#) qui : fournit des fonctionnalités permettant de gérer les liens d'Observability Access Manager et d'établir le partage des ressources des CloudWatch journaux

Utilisation de cette stratégie

Vous pouvez les associer CloudWatchLogsCrossAccountSharingConfiguration à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 13:55 UTC
- Heure modifiée : 27 novembre 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam:DeleteLink",
      "oam:GetLink",
      "oam:TagResource"
    ],
    "Resource" : "arn:aws:oam:*:*:link/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam:CreateLink",
      "oam:UpdateLink"
    ],
    "Resource" : [
      "arn:aws:oam:*:*:link/*",
      "arn:aws:oam:*:*:sink/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchLogsFullAccess

CloudWatchLogsFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux CloudWatch journaux

Utilisation de cette politique

Vous pouvez vous associer CloudWatchLogsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 26 novembre 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchLogsReadOnlyAccess

CloudWatchLogsReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux CloudWatch journaux

Utilisation de cette politique

Vous pouvez vous associer CloudWatchLogsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 26 novembre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",

```

```
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchNetworkMonitorServiceRolePolicy

CloudWatchNetworkMonitorServiceRolePolicy est une [politique AWS gérée](#) qui : permet à CloudWatch Network Monitor d'accéder aux ressources EC2 et VPC et de les gérer, de publier des données et d'accéder CloudWatch à d'autres services requis en votre nom.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 21 décembre 2023, 18:53 UTC
- Heure modifiée : 21 décembre 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
```

```
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
    }
  }
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchReadOnlyAccess

CloudWatchReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à CloudWatch.

Utilisation de cette politique

Vous pouvez vous associer CloudWatchReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 5 décembre 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
      ]
    }
  ]
}
```

```
    "xray:Get*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OAMReadPermissions",
  "Effect" : "Allow",
  "Action" : [
    "oam:ListAttachedLinks"
  ],
  "Resource" : "arn:aws:oam:*:*:sink/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CloudWatchSyntheticsFullAccess

CloudWatchSyntheticsFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à CloudWatch Synthetics.

Utilisation de cette stratégie

Vous pouvez CloudWatchSyntheticsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 25 novembre 2019, 17:39 UTC
- Heure modifiée : 6 mai 2022, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Version de la politique

Version de la politique :v9 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "s3:GetBucketLocation"
],
"Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::cw-syn-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "synthetics.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
```

```
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch::*:alarm:Synthetics-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch::*:alarm:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:AddPermission",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration",
    "lambda:GetFunctionConfiguration",
    "lambda>DeleteFunction"
  ],
  "Resource" : [
    "arn:aws:lambda::*:function:cwsyn-*"
  ]
}
```

```
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetLayerVersion",
    "lambda:PublishLayerVersion",
    "lambda:DeleteLayerVersion"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:layer:cwsyn-*",
    "arn:aws:lambda:*:*:layer:Synthetics:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:Subscribe",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "arn:*:sns:*:*:Synthetics-*"
  ]
},
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

CloudWatchSyntheticsReadOnlyAccess

CloudWatchSyntheticsReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule à CloudWatch Synthetics.

Utilisation de cette stratégie

Vous pouvez CloudWatchSyntheticsReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails de la stratégie

- Type : politique AWS gérée
- Heure de création : 25 novembre 2019, 17:45 UTC
- Heure modifiée : 6 mars 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ComprehendDataAccessRolePolicy

ComprehendDataAccessRolePolicyest une [politiqueAWS gérée qui : Politique](#) relative au rôle de serviceAWS Comprehend qui permet d'accéder aux ressources S3 pour l'accès aux données

Utilisation de cette stratégie

Vous pouvezComprehendDataAccessRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 mars 2019, 22:28 UTC
- Heure modifiée : 6 mars 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : {
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::*Comprehend*",
    "arn:aws:s3::*comprehend*"
  ]
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ComprehendFullAccess

ComprehendFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Comprehend.

Utilisation de cette stratégie

Vous pouvez les associer ComprehendFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2017, 18:08 UTC
- Heure modifiée : 5 décembre 2017, 01:36 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ComprehendMedicalFullAccess

ComprehendMedicalFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à Amazon Comprehend Medical

Utilisation de cette stratégie

Vous pouvez `ComprehendMedicalFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 17:55 UTC
- Heure modifiée : 27 novembre 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ComprehendReadOnly

ComprehendReadOnly est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à Amazon Comprehend.

Utilisation de cette stratégie

Vous pouvez ComprehendReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2017, 18:10 UTC
- Heure modifiée : 26 avril 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Version de la politique

Version de la politique :v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",

```

```

    "comprehend:BatchDetectKeyPhrases",
    "comprehend:DetectPiiEntities",
    "comprehend:ContainsPiiEntities",
    "comprehend:DetectSentiment",
    "comprehend:BatchDetectSentiment",
    "comprehend:DetectSyntax",
    "comprehend:BatchDetectSyntax",
    "comprehend:ClassifyDocument",
    "comprehend:DescribeTopicsDetectionJob",
    "comprehend:ListTopicsDetectionJobs",
    "comprehend:DescribeDominantLanguageDetectionJob",
    "comprehend:ListDominantLanguageDetectionJobs",
    "comprehend:DescribeEntitiesDetectionJob",
    "comprehend:ListEntitiesDetectionJobs",
    "comprehend:DescribeKeyPhrasesDetectionJob",
    "comprehend:ListKeyPhrasesDetectionJobs",
    "comprehend:DescribePiiEntitiesDetectionJob",
    "comprehend:ListPiiEntitiesDetectionJobs",
    "comprehend:DescribeSentimentDetectionJob",
    "comprehend:DescribeTargetedSentimentDetectionJob",
    "comprehend:ListSentimentDetectionJobs",
    "comprehend:ListTargetedSentimentDetectionJobs",
    "comprehend:DescribeDocumentClassifier",
    "comprehend:ListDocumentClassifiers",
    "comprehend:DescribeDocumentClassificationJob",
    "comprehend:ListDocumentClassificationJobs",
    "comprehend:DescribeEntityRecognizer",
    "comprehend:ListEntityRecognizers",
    "comprehend:ListTagsForResource",
    "comprehend:DescribeEndpoint",
    "comprehend:ListEndpoints",
    "comprehend:ListDocumentClassifierSummaries",
    "comprehend:ListEntityRecognizerSummaries",
    "comprehend:DescribeResourcePolicy"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ComputeOptimizerReadOnlyAccess

ComputeOptimizerReadOnlyAccess est un [AWSpolitique gérée](#) qui : fournit un accès en lecture seule à ComputeOptimizer.

Utilisation de cette politique

Vous pouvez joindre ComputeOptimizerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type:AWSpolitique gérée
- Heure de création: 07 mars 2020, 00h11 UTC
- Heure modifiée :28 août 2023, 19 h 22 UTC
- ARN: arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

Version de la politique

Version de la politique : v7(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Action" : [  
  "compute-optimizer:DescribeRecommendationExportJobs",  
  "compute-optimizer:GetEnrollmentStatus",  
  "compute-optimizer:GetEnrollmentStatusesForOrganization",  
  "compute-optimizer:GetRecommendationSummaries",  
  "compute-optimizer:GetEC2InstanceRecommendations",  
  "compute-optimizer:GetEC2RecommendationProjectedMetrics",  
  "compute-optimizer:GetAutoScalingGroupRecommendations",  
  "compute-optimizer:GetEBSVolumeRecommendations",  
  "compute-optimizer:GetLambdaFunctionRecommendations",  
  "compute-optimizer:GetRecommendationPreferences",  
  "compute-optimizer:GetEffectiveRecommendationPreferences",  
  "compute-optimizer:GetECSServiceRecommendations",  
  "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",  
  "compute-optimizer:GetLicenseRecommendations",  
  "ec2:DescribeInstances",  
  "ec2:DescribeVolumes",  
  "ecs:ListServices",  
  "ecs:ListClusters",  
  "autoscaling:DescribeAutoScalingGroups",  
  "autoscaling:DescribeAutoScalingInstances",  
  "lambda:ListFunctions",  
  "lambda:ListProvisionedConcurrencyConfigs",  
  "cloudwatch:GetMetricData",  
  "organizations:ListAccounts",  
  "organizations:DescribeOrganization",  
  "organizations:DescribeAccount"  
],  
  "Resource" : "*"   
}   
]   
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

ComputeOptimizerServiceRolePolicy

ComputeOptimizerServiceRolePolicy est une [politique AWS gérée](#) qui : Permet d'ComputeOptimizer appeler les AWS services et de collecter des informations sur la charge de travail en votre nom.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 3 décembre 2019, 08:45 UTC
- Heure modifiée : 13 juin 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON Document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ConfigConformsServiceRolePolicy

ConfigConformsServiceRolePolicy est une [politiqueAWS gérée](#) qui : Politique requise pour AWSConfig créer des packs de conformité

Utilisation de cette politique de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles attachés à vos groupes ou les rôles attachés à d'autres groupes ou

Les détails des politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 25 juillet 2019, 21:38 UTC
- Heure modifiée : 12 janvier 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "config:PutConfigRule",
      "config>DeleteConfigRule"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeConfigRules"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeRemediationConfigurations",
      "config>DeleteRemediationConfiguration",
      "config:PutRemediationConfigurations"
    ],
    "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "remediation.config.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:GetObject",
      "s3:GetBucketAcl"
    ],
    "Resource" : "arn:aws:s3:::awsconfigconforms*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStackResources",

```

```

    "cloudformation:DescribeStacks",
    "cloudformation:GetStackPolicy",
    "cloudformation:SetStackPolicy",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateTerminationProtection",
    "cloudformation:ValidateTemplate",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Config"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques et évoluez avec AWS politiques de moindre privilège des autorisations de moindre privilège de privilège des autorisations de moindre privilège de privilège](#)

CostOptimizationHubAdminAccess

CostOptimizationHubAdminAccess est une [politique AWS gérée](#) qui : Cette politique gérée fournit un accès administrateur au Cost Optimization Hub.

Utilisation de cette politique

Vous pouvez vous associer CostOptimizationHubAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 décembre 2023, 00:03 UTC
- Heure modifiée : 19 décembre 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
    }
  ]
}
```

```

    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "organizations:ServicePrincipal" : [
          "cost-optimization-hub.bcm.amazonaws.com"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CostOptimizationHubReadOnlyAccess

CostOptimizationHubReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique gérée fournit un accès en lecture seule au Cost Optimization Hub.

Utilisation de cette politique

Vous pouvez vous associer `CostOptimizationHubReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 décembre 2023, 18:04 UTC
- Heure modifiée : 13 décembre 2023, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CostOptimizationHubServiceRolePolicy

CostOptimizationHubServiceRolePolicy est une [politique AWS gérée](#) qui : permet à Cost Optimization Hub de récupérer des informations sur l'organisation et de collecter des données et des métadonnées liées à l'optimisation.

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 26 novembre 2023, 08:03 UTC
- Heure modifiée : 26 novembre 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AwsOrgsAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListParents",
      "organizations:DescribeOrganizationalUnit"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "CostExplorerAccess",
    "Effect" : "Allow",
    "Action" : [
      "ce:ListCostAllocationTags"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

CustomerProfilesServiceLinkedRolePolicy

CustomerProfilesServiceLinkedRolePolicy est une [politique AWS gérée](#) qui : autorise les profils clients Amazon Connect à accéder aux AWS services et aux ressources en votre nom.

Utilisation de de de de de de de

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

détails les détails les détails

- Type : Politique de rôles liée à un service
- Heure de création : 7 mars 2023, 22:56 UTC
- Heure modifiée : 7 mars 2023, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/`
`CustomerProfilesServiceLinkedRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec](#)

DatabaseAdministrator

DatabaseAdministrator est une [politique AWS gérée](#) qui : accorde des autorisations d'accès complètes aux AWS services et aux actions nécessaires à la mise en place et à la configuration des services AWS de base de données.

Utilisation de cette stratégie

Vous pouvez DatabaseAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique relative aux fonctions Job
- Heure de création : 10 novembre 2016, 17:25 UTC
- Heure modifiée : 8 janvier 2019, 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline>DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda>DeleteEventSourceMapping",
        "lambda>DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
```



```

    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents",
    "logs:Create*",
    "logs:PutLogEvents",
    "logs:PutMetricFilter",
    "rds:*",
    "redshift:*",
    "s3:CreateBucket",
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:Get*",
    "sns:List*",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutBucketWebsite",
    "s3:PutLifecycleConfiguration",
    "s3:PutReplicationConfiguration",
    "s3:PutObject*",
    "s3:Replicate*",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [

```

```
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/rds-monitoring-role",
    "arn:aws:iam::*:role/rdbms-lambda-access",
    "arn:aws:iam::*:role/lambda_exec_role",
    "arn:aws:iam::*:role/lambda-dynamodb-*",
    "arn:aws:iam::*:role/lambda-vpc-execution-role",
    "arn:aws:iam::*:role/DataPipelineDefaultRole",
    "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

DataScientist

DataScientist est une [politique AWS gérée](#) qui : accorde des autorisations aux services d'analyse de données AWS.

Utilisation de cette stratégie

Vous pouvez les associer DataScientist à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique relative aux fonctions Job
- Heure de création : 10 novembre 2016, 17:28 UTC
- Heure modifiée : 3 décembre 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-fonction/DataScientist`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
```

```
    "iam:ListRoles",
    "kinesis:*",
    "kms:List*",
    "lambda:Create*",
    "lambda>Delete*",
    "lambda:Get*",
    "lambda:InvokeFunction",
    "lambda:PublishVersion",
    "lambda:Update*",
    "lambda:List*",
    "machinelearning:*",
    "sdb:*",
    "rds:*",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "redshift:*",
    "s3:CreateBucket",
    "sns:CreateTopic",
    "sns:Get*",
    "sns:List*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:Abort*",
    "s3>DeleteObject",
    "s3:Get*",
    "s3:List*",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketCors",
    "s3:PutBucketLogging",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:Replicate*",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "*"
  ]
}
```

```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DataPipelineDefaultRole",
      "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
      "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "arn:aws:iam::*:role/EMR_DefaultRole",
      "arn:aws:iam::*:role/kinesis-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:*"
    ],
    "NotResource" : [
      "arn:aws:sagemaker::*:domain/*",

```

```

    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:app/*",
    "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreatePresignedDomainUrl",
    "sagemaker:DescribeDomain",
    "sagemaker:ListDomains",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListUserProfiles",
    "sagemaker:*App",
    "sagemaker:ListApps"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:*FlowDefinition",
    "sagemaker:*FlowDefinitions"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "sagemaker:WorkteamType" : [
        "private-crowd",
        "vendor-crowd"
      ]
    }
  }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

DAXServiceRolePolicy

DAXServiceRolePolicy est une [politiqueAWS gérée](#) qui : Cette politique permet à DAX de créer et de gérer une interface réseau, un groupe de sécurité, un sous-réseau et un VPC pour le compte du client

Utilisation de de de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. You cannot attach this policy to your users, groups, or roles.

des des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 5 mars 2018, 17:51 UTC
- Heure modifiée : 5 mars 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version de stratégie Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

de stratégie de politique de JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
```

```
    "ec2:CreateSecurityGroup",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteSecurityGroup",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [stratégies AWS gérées](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy est une [politique AWS gérée](#) qui : Autorisations requises pour prendre en charge Amazon CloudWatch Contributor Insights pour Amazon DynamoDB.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 15 novembre 2019, 21:13 UTC
- Heure modifiée : 15 novembre 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy est une [politique AWS gérée](#) qui : Fournit à AWS DynamoDB un accès à KinesisDataStreams

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 novembre 2020, 00:43 UTC
- Heure modifiée : 12 novembre 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
```

```
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy est une [politique AWS gérée](#) qui : Autorisations requises par DynamoDB pour la réplication de données entre régions

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 09 novembre 2017, 23:55 UTC
- Heure modifiée : 8 janvier 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb>DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    }  
  }  
} ]  
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy est une [politique AWS gérée](#) qui : La politique autorise ec2fastlaunch à préparer et à gérer des instantanés préprovisionnés sur le compte du client et à publier les statistiques associées.

Utilisation

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 10 janvier 2022
- Heure modifiée : 10 janvier 2022, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [DémarrerAWS](#)

EC2FleetTimeShiftableServiceRolePolicy

EC2FleetTimeShiftableServiceRolePolicy est une [politique AWS gérée](#) qui : Politique accordant des autorisations à EC2 Fleet pour lancer des instances à l'future.

Utilisation des stratégies

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des

- Type : Politique de rôles liée à un service
- Heure de création : 23 décembre 2019
- Heure modifiée : 23 décembre 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de

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

```
]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS Démarrer avec](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Ec2ImageBuilderCrossAccountDistributionAccess est une [politique AWS gérée](#) qui :
Autorisations requises par EC2 Image Builder pour effectuer une distribution entre comptes.

Utilisation de cette stratégie

Vous pouvez Ec2ImageBuilderCrossAccountDistributionAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 19:22 UTC
- Heure modifiée : 30 septembre 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*::image/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:CopyImage",
      "ec2:ModifyImageAttribute"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

EC2ImageBuilderLifecycleExecutionPolicy

EC2ImageBuilderLifecycleExecutionPolicy est une [politique AWS gérée qui](#) : [La politique EC2 ImageBuilderLifecycleExecutionPolicy](#) autorise Image Builder à effectuer des actions telles que la désapprobation ou la suppression des ressources d'image Image Builder et de leurs ressources sous-jacentes (AMI, instantanés) afin de prendre en charge les règles automatisées relatives aux tâches de gestion du cycle de vie des images.

Utilisation de cette politique

Vous pouvez vous associer EC2ImageBuilderLifecycleExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 16 novembre 2023, 23:23 UTC
- Heure modifiée : 16 novembre 2023, 23h23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
  ],
}
```

```

    "Sid" : "EC2DeleteSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "EC2TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*::snapshot/*",
      "arn:aws:ec2:*::image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "DeprecatedBy"
      }
    }
  },
  {
    "Sid" : "ECRIImagePermission",
    "Effect" : "Allow",
    "Action" : [
      "ecr:BatchGetImage",
      "ecr:BatchDeleteImage"
    ],
    "Resource" : "arn:aws:ecr:*::repository/*",
    "Condition" : {
      "StringEquals" : {
        "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
      }
    }
  }
}

```

```
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

EC2InstanceConnect

EC2InstanceConnect est une [politique AWS gérée](#) qui : permet aux clients d'appeler EC2 Instance Connect pour publier des clés éphémères vers leurs instances EC2 et se connecter via SSH ou l'interface de ligne de commande EC2 Instance Connect.

Utilisation de cette stratégie

Vous pouvez EC2InstanceConnect les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 juin 2019, 18:53 UTC
- Heure modifiée : 27 juin 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

Ec2InstanceConnectEndpoint

Ec2InstanceConnectEndpoint est une [politique AWS gérée](#) qui : [politique](#) de point de terminaison EC2 Instance Connect pour gérer les points de terminaison EC2 Instance Connect créés par le client

Utilisation des stratégies

Cette politique est attachée à un rôle lié à un service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 24 janvier 2023, 20:19 UTC
- Heure modifiée : 24 janvier 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "InstanceConnectEndpointId"
      ]
    },
    "Null" : {
      "aws:RequestTag/InstanceConnectEndpointId" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/InstanceConnectEndpointId" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "InstanceConnectEndpointId"
      ]
    }
  }
},
```

```
    "Null" : {
      "aws:RequestTag/InstanceConnectEndpointId" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/InstanceConnectEndpointId" : [
          "eice-*"
        ]
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez les autorisations de moindre privilège](#)

EC2InstanceProfileForImageBuilder

EC2InstanceProfileForImageBuilder est une [politiqueAWS gérée](#) qui : profil d'instance EC2 pour le service Image Builder.

Utilisation de cette stratégie

Vous pouvez EC2InstanceProfileForImageBuilder les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée

- Heure de création : 1 décembre 2019, 19:08 UTC
- Heure modifiée : 27 août 2020, 16:40 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
```

```
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::ec2imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

EC2InstanceProfileForImageBuilderECRContainerBuilds est une [politique AWS gérée](#) qui : profil d'instance EC2 pour la création d'images de conteneurs avec EC2 Image Builder. Cette politique accorde à l'utilisateur de larges autorisations pour télécharger des images ECR.

Utilisation de cette stratégie

Vous pouvez EC2InstanceProfileForImageBuilderECRContainerBuilds les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 11 décembre 2020, 19:48 UTC

- Heure modifiée : 11 décembre 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
        "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
        "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
        ]
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::ec2imagebuilder*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ECRReplicationServiceRolePolicy

ECRReplicationServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise l'accès Services AWS aux ressources utilisées ou gérées par ECR Replication

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 4 décembre 2020, 22h11 UTC
- Heure modifiée : 4 décembre 2020, 22h11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElastiCacheServiceRolePolicy

ElastiCacheServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique permet de ElastiCache gérer les AWS ressources en votre nom selon les besoins de gestion de votre cache

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 07 décembre 2017, 17:50 UTC
- Heure modifiée : 28 novembre 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:RevokeSecurityGroupIngress",
      "cloudwatch:PutMetricData",
      "outposts:GetOutpost",
      "outposts:GetOutpostInstanceTypes",
      "outposts:ListOutposts",
      "outposts:ListSites"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateDeleteVPCEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringLike" : {
        "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
      }
    }
  },
  {
    "Sid" : "TagVPCEndpointsOnCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",

```

```
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AmazonElasticCacheManaged" : "true"
      }
    }
  },
  {
    "Sid" : "ModifyVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AmazonElasticCacheManaged" : "true"
      }
    }
  },
  {
    "Sid" : "AllowAccessToElasticCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2:ModifyVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
  }
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ElasticLoadBalancingFullAccess

ElasticLoadBalancingFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon ElasticLoadBalancing et un accès limité aux autres services nécessaires à la fourniture de ElasticLoadBalancing fonctionnalités.

Utilisation de cette stratégie

Vous pouvez ElasticLoadBalancingFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 20 septembre 2018, 20:42 UTC
- Heure modifiée : 29 novembre 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Version de la politique

Version de la politique :v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeClassicLinkInstances",
    "ec2:DescribeRouteTables",
    "ec2:DescribeCoipPools",
    "ec2:GetCoipPoolUsage",
    "ec2:DescribeVpcPeeringConnections",
    "cognito-idp:DescribeUserPoolClient"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "arc-zonal-shift:*",
  "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "arc-zonal-shift:ListManagedResources",
    "arc-zonal-shift:ListZonalShifts"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElasticLoadBalancingReadOnly

ElasticLoadBalancingReadOnlyest une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon ElasticLoadBalancing et aux services dépendants

Utilisation de cette politique

Vous pouvez vous associer ElasticLoadBalancingReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 septembre 2018, 20:17 UTC
- Heure modifiée : 26 novembre 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Sid" : "Statement1",
"Effect" : "Allow",
"Action" : [
  "elasticloadbalancing:Describe*",
  "elasticloadbalancing:Get*"
],
"Resource" : "*"
},
{
  "Sid" : "Statement2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeClassicLinkInstances",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Statement3",
  "Effect" : "Allow",
  "Action" : "arc-zonal-shift:GetManagedResource",
  "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
},
{
  "Sid" : "Statement4",
  "Effect" : "Allow",
  "Action" : [
    "arc-zonal-shift:ListManagedResources",
    "arc-zonal-shift:ListZonalShifts"
  ],
  "Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ElementalActivationsDownloadSoftwareAccess

ElementalActivationsDownloadSoftwareAccess est une [politique AWS gérée](#) qui : permet de consulter les actifs achetés et de télécharger les logiciels associés et les fichiers Kickstart

Utilisation de cette stratégie

Vous pouvez ElementalActivationsDownloadSoftwareAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 8 septembre 2020, 17:26 UTC
- Heure modifiée : 8 septembre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalActivationsFullAccess

ElementalActivationsFullAccess est une [politiqueAWS gérée](#) qui : Accès complet permettant de visualiser et de prendre des mesures sur les actifs achetés sur les appliances et les logiciels Elemental

Utilisation de cette stratégie

Vous pouvez ElementalActivationsFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 4 juin 2020, 21:00 UTC
- Heure modifiée : 4 juin 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalActivationsGenerateLicenses

ElementalActivationsGenerateLicenses est une [politique AWS gérée](#) qui : permet de consulter les actifs achetés et de générer des licences logicielles pour les activations en attente

Utilisation de cette stratégie

Vous pouvez ElementalActivationsGenerateLicenses les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 août 2020, 18:28 UTC
- Heure modifiée : 28 août 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalActivationsReadOnlyAccess

ElementalActivationsReadOnlyAccess est une [politique AWS gérée](#) qui : Accès en lecture seule à la liste détaillée des actifs achetés associés à Compte AWS l'utilisateur

Utilisation de cette stratégie

Vous pouvez les associer `ElementalActivationsReadOnlyAccess` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 28 août 2020, 16:51 UTC
- Heure modifiée : 28 août 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalAppliancesSoftwareFullAccess

ElementalAppliancesSoftwareFullAccess est une [politique AWS gérée](#) qui : Accès complet à la consultation et à la prise de mesures concernant les devis et les commandes des appliances et logiciels Elemental

Utilisation de cette stratégie

Vous pouvez ElementalAppliancesSoftwareFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 31 juillet 2019, 16:28 UTC
- Heure modifiée : 5 février 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "elemental-appliances-software:*",
      "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalAppliancesSoftwareReadOnlyAccess

ElementalAppliancesSoftwareReadOnlyAccess est une [politique AWS gérée](#) qui : Accès en lecture seule pour consulter les devis et les commandes des appliances et logiciels Elemental

Utilisation de cette stratégie

Vous pouvez les associer ElementalAppliancesSoftwareReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 1 avril 2020, 22:31 UTC
- Heure modifiée : 01 avril 2020, 22:31 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ElementalSupportCenterFullAccess

ElementalSupportCenterFullAccess est une [politique AWS gérée](#) qui : Accès complet permettant de consulter les dossiers de support des applications et des logiciels Elemental et de prendre des mesures à leur sujet, ainsi que le contenu de support produit

Utilisation de cette stratégie

Vous pouvez ElementalSupportCenterFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 novembre 2020, 18:08 UTC
- Heure modifiée : 5 février 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL est une [politique AWS gérée](#) qui : Cette politique accorde des autorisations en lecture seule qui permettent au service WAL pour Amazon EMR de rechercher et de renvoyer l'état d'un cluster

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas associer cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 15 juin 2023, 23:30 UTC
- Heure modifiée : 15 juin 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

FMSServiceRolePolicy

FMSServiceRolePolicy est une [politique AWS gérée qui : Politique](#) d'accès permettant à un rôle lié au service FM d'effectuer des actions liées à la FM sur les ressources gérées par la FM au sein d'un compte d'AWS organisation client.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 28 mars 2018, 23:01 UTC
- Heure modifiée : 21 avril 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Version de la politique

Version de la politique :v28 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*:*/restapis/*/stages/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2>DeleteLoggingConfiguration"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:regional/webacl/*",
      "arn:aws:wafv2:*:*:global/webacl/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "waf:CreateWebACL",
      "waf-regional:CreateWebACL",
      "waf:GetChangeToken",
      "waf-regional:GetChangeToken",
      "waf-regional:GetWebACLForResource"
    ],
    "Resource" : [
      "arn:aws:waf:*:*:*",
      "arn:aws:waf-regional:*:*:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
      "elasticloadbalancing:DescribeTags"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "waf:PutPermissionPolicy",
      "waf:GetPermissionPolicy",
      "waf>DeletePermissionPolicy",
      "waf-regional:PutPermissionPolicy",
      "waf-regional:GetPermissionPolicy",
      "waf-regional>DeletePermissionPolicy"
    ],
    "Resource" : [
      "arn:aws:waf:*:*:webacl/*",
      "arn:aws:waf:*:*:rulegroup/*",
      "arn:aws:waf-regional:*:*:webacl/*",
      "arn:aws:waf-regional:*:*:rulegroup/*"
    ]
  }
]

```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config>DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/"
    }
  ],
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeComplianceByConfigRule",
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config:PutConfigurationRecorder",
      "config:StartConfigurationRecorder",
      "config:PutDeliveryChannel",
      "config:DescribeDeliveryChannels",
      "config:DescribeDeliveryChannelStatus",
      "config:GetComplianceSummaryByConfigRule",
      "config:GetDiscoveredResourceCounts",
      "config:PutEvaluations",
      "config>SelectResourceConfig"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",

```

```
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "config:DescribeConfigRuleEvaluationStatus",
    "config:DescribeConfigRules",
    "organizations:ListAccounts",
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListChildren",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "shield:CreateProtection",
    "shield>DeleteProtection",
    "shield:DescribeProtection",
    "shield>ListProtections",
    "shield>ListAttacks",
    "shield>CreateSubscription",
    "shield:DescribeSubscription",
    "shield:GetSubscriptionState",
    "shield:DescribeDRTAccess",
    "shield:DescribeEmergencyContactSettings",
    "shield:UpdateEmergencyContactSettings",
    "elasticloadbalancing:DescribeLoadBalancers",
    "ec2:DescribeAddresses",
    "shield:EnableApplicationLayerAutomaticResponse",
    "shield:DisableApplicationLayerAutomaticResponse",
    "shield:UpdateApplicationLayerAutomaticResponse"
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2>DeleteSecurityGroup",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
      "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeInstances"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  },
  {
    "Effect" : "Allow",
```



```

    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/FMManaged" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeStaleSecurityGroups",
      "ec2:DescribeNetworkInterfaces",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "wafv2:TagResource",
      "wafv2:ListResourcesForWebACL",
      "wafv2:AssociateWebACL",
      "wafv2:ListTagsForResource",
      "wafv2:UntagResource",
      "wafv2:GetWebACL",
      "wafv2:DisassociateFirewallManager",
      "wafv2>DeleteWebACL",
      "wafv2:DisassociateWebACL"
    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:global/webacl/*",

```

```

    "arn:aws:wafv2:*:*:regional/webacl/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:UpdateWebACL",
    "wafv2:CreateWebACL",
    "wafv2>DeleteFirewallManagerRuleGroups",
    "wafv2:PutFirewallManagerRuleGroups"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/webacl/*",
    "arn:aws:wafv2:*:*:regional/webacl/*",
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*",
    "arn:aws:wafv2:*:*:global/managedruleset/*",
    "arn:aws:wafv2:*:*:regional/managedruleset/*",
    "arn:aws:wafv2:*:*:global/ipset/*",
    "arn:aws:wafv2:*:*:regional/ipset/*",
    "arn:aws:wafv2:*:*:global/regexpatternset/*",
    "arn:aws:wafv2:*:*:regional/regexpatternset/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutPermissionPolicy",
    "wafv2:GetPermissionPolicy",
    "wafv2>DeletePermissionPolicy"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:ListTagsForResource"
  ],
  "Resource" : "*"
},
{

```

```
"Effect" : "Allow",
"Action" : [
  "wafv2:GetWebACLForResource"
],
"Resource" : [
  "arn:aws:wafv2:*:*:regional/webacl/*"
]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateRouteTable"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:DeleteRouteTable",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateRouteTable",
      "ec2>DeleteSubnet",
      "ec2:DisassociateRouteTable",
      "ec2:ReplaceRouteTableAssociation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInternetGateways",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSubnets",
      "ec2:DescribeTags",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeAvailabilityZones"
    ]
  }
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : [
          "true"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ram:TagResource"
    ],
    "Resource" : [
      "arn:aws:ram:*:*:resource-share/*"
    ]
  }
}
```

```
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceShare",
      "ram:UpdateResourceShare",
      "ram>DeleteResourceShare"
    ],
    "Resource" : "arn:aws:ram:*:*:resource-share/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ram:CreateResourceShare",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      },
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : [
          "true"
        ]
      }
    }
  },
  {
    "Sid" : "ram",
```

```
"Effect" : "Allow",
"Action" : [
  "ram:GetResourceShareAssociations",
  "ram:GetResourceShares"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "network-firewall.amazonaws.com",
        "shield.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:AssociateSubnets",
```

```

    "network-firewall:CreateFirewall",
    "network-firewall:CreateFirewallPolicy",
    "network-firewall:DisassociateSubnets",
    "network-firewall:UpdateFirewallDeleteProtection",
    "network-firewall:UpdateFirewallPolicy",
    "network-firewall:UpdateFirewallPolicyChangeProtection",
    "network-firewall:UpdateSubnetChangeProtection",
    "network-firewall:AssociateFirewallPolicy",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "network-firewall:PutResourcePolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall>DeleteResourcePolicy",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:UpdateLoggingConfiguration"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "network-firewall>DeleteFirewallPolicy",
    "network-firewall>DeleteFirewall"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:ListLogDeliveries",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery"
  ],

```



```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53resolver:ListFirewallRuleGroupAssociations",
      "route53resolver:ListTagsForResource",
      "route53resolver:ListFirewallRuleGroups",
      "route53resolver:GetFirewallRuleGroupAssociation",
      "route53resolver:GetFirewallRuleGroup",
      "route53resolver:GetFirewallRuleGroupPolicy",
      "route53resolver:PutFirewallRuleGroupPolicy"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53resolver:UpdateFirewallRuleGroupAssociation",
      "route53resolver:DisassociateFirewallRuleGroup"
    ],
    "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53resolver:AssociateFirewallRuleGroup",
      "route53resolver:TagResource"
    ],
    "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : "true"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess est une [politiqueAWS gérée](#) qui : Permet à Amazon FSx de supprimer ses rôles liés aux services pour accéder à Amazon S3

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique ou à un utilisateur ou un ou un rôle ou un rôle ou un rôle ou un rôle.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 28 novembre 2018, 10:40 UTC
- Heure modifiée : 28 novembre 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:GetRole"
    ],
    "Resource" : "arn:*:iam:*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

GameLiftGameServerGroupPolicy

GameLiftGameServerGroupPolicy est une [politique AWS gérée](#) qui : Politique permettant à Gamelift de GameServerGroups gérer les ressources des clients

Utilisation de cette stratégie

Vous pouvez GameLiftGameServerGroupPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 3 avril 2020, 23h12 UTC
- Heure modifiée : 13 mai 2020, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

Version de la politique

Version de la politique :v3 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
```

```
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "sns:Publish",
  "Resource" : [
    "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
    "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/GameLift"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

GlobalAcceleratorFullAccess

GlobalAcceleratorFullAccess est une [politique AWS gérée](#) qui : Autorise GlobalAccelerator les utilisateurs à accéder pleinement à toutes les API

Utilisation de cette stratégie

Vous pouvez `GlobalAcceleratorFullAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 02:44 UTC
- Heure modifiée : 4 décembre 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
```

```
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeRegions",
    "ec2:DescribeSubnets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

GlobalAcceleratorReadOnlyAccess

GlobalAcceleratorReadOnlyAccess est une [politique AWS gérée](#) qui : Autorise GlobalAccelerator les utilisateurs à accéder aux API en lecture seule

Utilisation de cette stratégie

Vous pouvez GlobalAcceleratorReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2018, 02:41 UTC
- Heure modifiée : 27 novembre 2018, 02:41 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

GreengrassOTAUpdateArtifactAccess

GreengrassOTAUpdateArtifactAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture aux artefacts de Greengrass OTA Update dans toutes les régions de Greengrass

Utilisation de cette stratégie

Vous pouvez GreengrassOTAUpdateArtifactAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 29 novembre 2017, 18:11 UTC
- Heure modifiée : 18 décembre 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*-greengrass-updates/*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

GroundTruthSyntheticConsoleFullAccess

GroundTruthSyntheticConsoleFullAccess est une [politiqueAWS gérée](#) qui : Cette politique accorde les autorisations nécessaires pour utiliser toutes les fonctionnalités de la console synthétique SageMaker Ground Truth.

Utilisation de cette stratégie

Vous pouvez les associerGroundTruthSyntheticConsoleFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 25 août 2022, 15:58 UTC
- Heure modifiée : 25 août 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

GroundTruthSyntheticConsoleReadOnlyAccess

GroundTruthSyntheticConsoleReadOnlyAccess est une [politique AWS gérée](#) qui : Cette politique accorde un accès en lecture seule à SageMaker Ground Truth Synthetic via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez GroundTruthSyntheticConsoleReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 25 août 2022, 15:58 UTC

- Heure modifiée : 25 août 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

Health_OrganizationsServiceRolePolicy

Health_OrganizationsServiceRolePolicy est une [politique AWS gérée qui : Politique](#) de AWS santé pour activer la fonctionnalité Organizational View

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 16 décembre 2019, 13:28 UTC
- Heure modifiée : 6 février 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
      ]
    }
  ]
}
```

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

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

IAMAccessAdvisorReadOnly

IAMAccessAdvisorReadOnly est une [politiqueAWS gérée](#) qui : Cette politique permet de lire toutes les informations d'accès fournies par le conseiller d'accès IAM, telles que les informations relatives au dernier accès au service.

Utilisation de cette stratégie

Vous pouvez les associer IAMAccessAdvisorReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 21 juin 2019, 19:33 UTC
- Heure modifiée : 21 juin 2019, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMAccessAnalyzerFullAccess

IAMAccessAnalyzerFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à IAM Access Analyzer

Utilisation de cette stratégie

Vous pouvez les associer IAMAccessAnalyzerFullAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 2 décembre 2019, 17:12 UTC
- Heure modifiée : 2 décembre 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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



```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:ListAccounts",
      "organizations:ListAccountsForParent",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListChildren",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListParents",
      "organizations:ListRoots"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMAccessAnalyzerReadOnlyAccess

IAMAccessAnalyzerReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux ressources d'IAM Access Analyzer

Utilisation de cette politique

Vous pouvez vous associer IAMAccessAnalyzerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 2 décembre 2019, 17:12 UTC
- Heure modifiée : 27 novembre 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

IAMFullAccess

IAMFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à IAM via le AWS Management Console.

Utilisation de cette stratégie

Vous pouvez IAMFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 21 juin 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMReadOnlyAccess

IAMReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à IAM via leAWS Management Console.

Utilisation de cette stratégie

Vous pouvezIAMReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:40 UTC
- Heure modifiée : 25 janvier 2018, 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMSelfManageServiceSpecificCredentials

IAMSelfManageServiceSpecificCredential est une [politique AWS gérée](#) qui : Permet à un utilisateur IAM de gérer ses propres informations d'identification spécifiques au service.

Utilisation de cette stratégie

Vous pouvez IAMSelfManageServiceSpecificCredentials les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 22 décembre 2016, 17:25 UTC
- Heure modifiée : 22 décembre 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam>DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMUserChangePassword

IAMUserChangePassword est une [politique AWS gérée](#) qui : permet à un utilisateur IAM de modifier son propre mot de passe.

Utilisation de cette stratégie

Vous pouvez les associer IAMUserChangePassword à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 15 novembre 2016, 00:25 UTC
- Heure modifiée : 15 novembre 2016, 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

IAMUserSSHKeys

IAMUserSSHKeys est une [politique AWS gérée](#) qui : permet à un utilisateur IAM de gérer ses propres clés SSH.

Utilisation de cette stratégie

Vous pouvez IAMUserSSHKeys les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 juillet 2015, 17:08 UTC
- Heure modifiée : 09 juillet 2015, 17:08 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

IVSFullAccess

IVSFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet au service vidéo interactif (IVS), inclut également des autorisations pour les services dépendants, nécessaires pour un accès complet à la console ivs.

Utilisation de cette politique

Vous pouvez vous associer IVSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 décembre 2023, 21:20 UTC
- Heure modifiée : 13 décembre 2023, 21h20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "IVSFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "ivs:*",
    "ivschat:*"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

IVSReadOnlyAccess

IVSReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux API IVS à faible latence et de streaming en temps réel

Utilisation de cette politique

Vous pouvez vous associer IVSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 décembre 2023, 18h00 UTC
- Heure modifiée : 16 février 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

IVSRecordToS3

IVSRecordToS3 est une [politique AWS gérée](#) qui : Rôle lié au service pour exécuter S3 PutObject afin d'enregistrer des flux en direct IVS

des politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Policy details

- Type : Politique de rôles liée à un service
- Heure de création : 5 décembre 2020, 00:10 UTC
- Heure modifiée : 5 décembre 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Version de la politique

Version de la politique :v1 (par défaut)

La version de politique est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

document de politique

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS](#)

KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique accorde à Kafka Connect l'autorisation de gérer AWS des ressources en votre nom.

Les politiques de cette politique de politique

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher de cette politique à des utilisateurs, des groupes ou des rôles à des utilisateurs, des groupes ou des rôles à des rôles

les politiques politiques politiques politiques

- Type : Politique de rôles liée à un service
- Heure de création : 7 septembre 2021, 13:12 UTC
- Heure modifiée : 07 septembre 2021, 13:12 UTC

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

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut des politiques de politique est la version qui définit des autorisations pour la stratégie de politique de politique de politique de politique de politique de politique est. Lorsque un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

JSON des politiques JSON des

```
{
  "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"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer des stratégies AWS gérées des stratégies gérées à évoluez vers les autorisations de moindre privilège et évoluez vers les autorisations de moindre privilège](#)

KafkaServiceRolePolicy

KafkaServiceRolePolicy est une [politique AWS gérée](#) qui : politique de rôle liée au service IAM pour Kafka.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 15 novembre 2018, 23:31 UTC
- Heure modifiée : 28 avril 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : "arn:*:ec2:*:*:subnet/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "ec2:ResourceTag/ClusterArn" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:DescribeSecret"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
    }
  }
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy est une [politiqueAWS gérée](#) qui : Autorisations requises par Keyspaces pour la réplication de données entre régions

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails politiques

- Type : Politique de rôles liée à un service
- Heure de création : 2 mai 2023, 16:15 UTC
- Heure modifiée : 2 mai 2023, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie son document de politique

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

```
    "Effect" : "Allow",
    "Action" : [
      "cassandra:Select",
      "cassandra:SelectMultiRegionResource",
      "cassandra:Modify",
      "cassandra:ModifyMultiRegionResource"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

LakeFormationDataAccessServiceRolePolicy

LakeFormationDataAccessServiceRolePolicy est une [politique AWS gérée](#) qui : Politique visant à accorder un accès temporaire aux données aux ressources de Lake Formation

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 20 juin 2019, 20:46 UTC
- Heure modifiée : 6 février 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

LexBotPolicy

LexBotPolicy est une [politique AWS gérée qui : Politique](#) pour le cas d'utilisation de AWS Lex Bot

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service

- Heure de création : 17 février 2017, 22:18 UTC
- Heure modifiée : 13 novembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

LexChannelPolicy

LexChannelPolicy est une [politiqueAWS gérée qui : Politique](#) pour le cas d'utilisation deAWS Lex Channel

Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation Utilisation

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 février 2017, 23:23 UTC
- Heure modifiée : 17 février 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

LightsailExportAccess

LightsailExportAccess est une [politiqueAWS gérée qui : Politique](#) de rôles liés au serviceAWS Lightsail qui accorde des autorisations pour exporter des ressources

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 28 septembre 2018, 16:35 UTC
- Heure modifiée : 15 janvier 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

MediaConnectGatewayInstanceRolePolicy

MediaConnectGatewayInstanceRolePolicy est une [politique AWS gérée](#) qui : Cette politique autorise l'enregistrement d'instances de MediaConnect passerelle auprès d'une MediaConnect passerelle.

Utilisation de cette stratégie

Vous pouvez MediaConnectGatewayInstanceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 22 mars 2023, 20:43 UTC
- Heure modifiée : 22 mars 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ]
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

MediaPackageServiceRolePolicy

MediaPackageServiceRolePolicy est une [politique AWS gérée](#) qui : Permet MediaPackage de publier des journaux sur CloudWatch

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 18 septembre 2020, 17:45 UTC
- Heure modifiée : 18 septembre 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

MemoryDBServiceRolePolicy

MemoryDBServiceRolePolicy est une [stratégie AWS gérée](#) qui : Cette stratégie permet à MemoryDB de gérer AWS des ressources en votre nom selon les besoins, en vue de gérer vos ressources.

Utilisation de cette politique

Cette stratégie est attachée à un rôle lié à un service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez attacher cette stratégie à vos utilisateurs, des groupes ou des rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 17 août 2021, 22:34 UTC
- Heure modifiée : 18 août 2021, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ]
}

```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/MemoryDB"
      }
    }
  }
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

MigrationHubDMSAccessServiceRolePolicy

MigrationHubDMSAccessServiceRolePolicy est une [politiqueAWS gérée](#) qui : [Politique](#) permettant au Database Migration Service d'assumer un rôle dans le compte du client pour appeler Migration Hub

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 juin 2019, 17:50 UTC
- Heure modifiée : 7 octobre 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```



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

```
    ]  
  }  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies de moindre moindre moindreAWS moindre moindre moindre moindre moindre moindre privilège d'moindre moindre privilège moindre privilège d'moindre moindre privilège moindre](#)

MigrationHubSMSAccessServiceRolePolicy

MigrationHubSMSAccessServiceRolePolicy est une [politiqueAWS gérée qui : Politique](#) permettant au service de migration des serveurs d'assumer un rôle dans le compte du client pour appeler Migration Hub

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 juin 2019, 18h30 UTC
- Heure modifiée : 7 octobre 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS et évoluez vers les autorisations de moindre privilège](#)

MonitronServiceRolePolicy

MonitronServiceRolePolicy est une [politiqueAWS gérée](#) qui : Politique relative au rôle lié au serviceAWS Monitron accordant l'accès aux ressources client requises.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les politiques

- Type : Politique de rôles liée à un service
- Heure de création : 2 mai 2022, 19:22 UTC
- Heure modifiée : 2 mai 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents"
],
"Resource" : [
  "arn:aws:logs:*:*:log-group:/aws/monitron/*"
]
}
]
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluées vers le moindre privilège](#)

NeptuneConsoleFullAccess

NeptuneConsoleFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet pour gérer Amazon Neptune à l'aide de l'AWS Management Console. Notez que cette politique accorde également un accès complet pour publier sur toutes les rubriques SNS du compte, des autorisations pour créer et modifier des instances Amazon EC2 et des configurations VPC, des autorisations pour afficher et répertorier les clés sur Amazon KMS, et un accès complet à Amazon RDS. Pour plus d'informations, consultez <https://aws.amazon.com/neptune/faqs/>.

Utilisation de cette politique

Vous pouvez vous associer NeptuneConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 juin 2018, 21:35 UTC
- Heure modifiée : 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds>CreateDBClusterParameterGroup",

```

```
"rds:CreateDBClusterSnapshot",
"rds:CreateDBParameterGroup",
"rds:CreateDBSubnetGroup",
"rds:CreateEventSubscription",
"rds>DeleteDBCluster",
"rds>DeleteDBClusterParameterGroup",
"rds>DeleteDBClusterSnapshot",
"rds>DeleteDBInstance",
"rds>DeleteDBParameterGroup",
"rds>DeleteDBSubnetGroup",
"rds>DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
```



```

    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowOtherDependentPermissions",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:AllocateAddress",
    "ec2:AssignIpv6Addresses",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:AssociateRouteTable",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AssociateVpcCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:CreateCustomerGateway",
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc",
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSubnet",
    "ec2:CreateVpc",
    "ec2:CreateVpcEndpoint",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAccountAttributes",

```

```

    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ModifyVpcEndpoint",
    "iam:ListRoles",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowPassRoleForNeptune",
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : "*"
}

```

```

    "Condition" : {
      "StringEquals" : {
        "iam:passedToService" : "rds.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowCreateSLRForNeptune",
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "rds.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
    "Effect" : "Allow",
    "Action" : [
      "neptune-graph:CreateGraph",
      "neptune-graph>DeleteGraph",
      "neptune-graph:GetGraph",
      "neptune-graph:ListGraphs",
      "neptune-graph:UpdateGraph",
      "neptune-graph:ResetGraph",
      "neptune-graph:CreateGraphSnapshot",
      "neptune-graph>DeleteGraphSnapshot",
      "neptune-graph:GetGraphSnapshot",
      "neptune-graph:ListGraphSnapshots",
      "neptune-graph:RestoreGraphFromSnapshot",
      "neptune-graph>CreatePrivateGraphEndpoint",
      "neptune-graph:GetPrivateGraphEndpoint",
      "neptune-graph:ListPrivateGraphEndpoints",
      "neptune-graph>DeletePrivateGraphEndpoint",
      "neptune-graph>CreateGraphUsingImportTask",
      "neptune-graph:GetImportTask",
      "neptune-graph:ListImportTasks",
      "neptune-graph:CancelImportTask"
    ],
    "Resource" : [
      "arn:aws:neptune-graph:*:*:*"
    ]
  }
}

```

```
    ]
  },
  {
    "Sid" : "AllowPassRoleForNeptuneAnalytics",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:passedToService" : "neptune-graph.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowCreateSLRForNeptuneAnalytics",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/AWSServiceRoleForNeptuneGraph",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

NeptuneFullAccess

NeptuneFullAccess est une [politique AWS gérée](#) qui : fournit un accès complet à Amazon Neptune. Notez que cette politique accorde également un accès complet pour publier sur toutes les

rubriques SNS du compte et un accès complet à Amazon RDS. Pour plus d'informations, consultez <https://aws.amazon.com/neptune/faqs/>.

Utilisation de cette politique

Vous pouvez vous associer NeptuneFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2018, 19:17 UTC
- Heure modifiée : 22 janvier 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
```

```
        "graphdb",
        "neptune"
    ]
}
},
{
  "Sid" : "AllowManagementPermissionsForRDS",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddRoleToDBCluster",
    "rds:AddSourceIdentifierToSubscription",
    "rds:AddTagsToResource",
    "rds:ApplyPendingMaintenanceAction",
    "rds:CopyDBClusterParameterGroup",
    "rds:CopyDBClusterSnapshot",
    "rds:CopyDBParameterGroup",
    "rds>CreateDBClusterEndpoint",
    "rds>CreateDBClusterParameterGroup",
    "rds>CreateDBClusterSnapshot",
    "rds>CreateDBParameterGroup",
    "rds>CreateDBSubnetGroup",
    "rds>CreateEventSubscription",
    "rds>CreateGlobalCluster",
    "rds>DeleteDBCluster",
    "rds>DeleteDBClusterEndpoint",
    "rds>DeleteDBClusterParameterGroup",
    "rds>DeleteDBClusterSnapshot",
    "rds>DeleteDBInstance",
    "rds>DeleteDBParameterGroup",
    "rds>DeleteDBSubnetGroup",
    "rds>DeleteEventSubscription",
    "rds>DeleteGlobalCluster",
    "rds:DescribeDBClusterEndpoints",
    "rds:DescribeAccountAttributes",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBClusterSnapshotAttributes",
    "rds:DescribeDBClusterSnapshots",
    "rds:DescribeDBClusters",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBLogFiles",
```

```
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:FailoverGlobalCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterEndpoint",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:ModifyGlobalCluster",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveFromGlobalCluster",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
"rds: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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

NeptuneGraphReadOnlyAccess

NeptuneGraphReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à toutes les ressources Amazon Neptune Analytics ainsi que des autorisations en lecture seule pour les services dépendants.

Utilisation de cette politique

Vous pouvez vous associer NeptuneGraphReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2023, 07:32 UTC

- Heure modifiée : 30 novembre 2023, 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
```

```
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

NeptuneReadOnlyAccess

NeptuneReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Neptune. Notez que cette politique accorde également l'accès aux ressources Amazon RDS. Pour plus d'informations, consultez <https://aws.amazon.com/neptune/faqs/>.

Utilisation de cette politique

Vous pouvez vous associer NeptuneReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2018, 19:16 UTC
- Heure modifiée : 22 janvier 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
```

```

    "rds:DescribeDBClusters",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBLogFiles",
    "rds:DescribeDBParameterGroups",
    "rds:DescribeDBParameters",
    "rds:DescribeDBSubnetGroups",
    "rds:DescribeEventCategories",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeEvents",
    "rds:DescribeGlobalClusters",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DownloadDBLogFilePortion",
    "rds:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForKMS",
  "Effect" : "Allow",

```

```

    "Action" : [
      "kms:ListKeys",
      "kms:ListRetirableGrants",
      "kms:ListAliases",
      "kms:ListKeyPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ]
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
    "Effect" : "Allow",
    "Action" : [
      "neptune-db:Read*",
      "neptune-db:Get*",
      "neptune-db:List*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

NetworkAdministrator

NetworkAdministrator est une [politique AWS gérée](#) qui : accorde des autorisations d'accès complètes aux AWS services et aux actions nécessaires à la mise en place et à la configuration des ressources AWS réseau.

Utilisation de cette stratégie

Vous pouvez NetworkAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique relative aux fonctions Job
- Heure de création : 10 novembre 2016, 17:31 UTC
- Heure modifiée : 16 septembre 2021, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*"
      ]
    }
  ]
}
```

```
"ec2:AcceptVpcEndpointConnections",
"ec2:AllocateAddress",
"ec2:AssignIpv6Addresses",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AssociateVpcCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVpnGateway",
"ec2:CreateCarrierGateway",
"ec2:CreateCustomerGateway",
"ec2:CreateDefaultSubnet",
"ec2:CreateDefaultVpc",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateFlowLogs",
"ec2:CreateInternetGateway",
"ec2:CreateNatGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkAclEntry",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreatePlacementGroup",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpcEndpointConnectionNotification",
"ec2:CreateVpcEndpointServiceConfiguration",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteCarrierGateway",
"ec2>DeleteEgressOnlyInternetGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
```



```
"ec2:DeletePlacementGroup",
"ec2:DeleteSubnet",
"ec2:DeleteTags",
"ec2:DeleteVpc",
"ec2:DeleteVpcEndpointConnectionNotifications",
"ec2:DeleteVpcEndpointServiceConfigurations",
"ec2:DeleteVpcEndpoints",
"ec2:DeleteVpnConnection",
"ec2:DeleteVpnConnectionRoute",
"ec2:DeleteVpnGateway",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
```

```
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeIpv6Pools",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:DisassociateSubnetCidrBlock",
"ec2:DisassociateVpcCidrBlock",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVpcClassicLinkDnsSupport",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVpcAttribute",
"ec2:ModifyVpcEndpoint",
"ec2:ModifyVpcEndpointConnectionNotification",
"ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:ModifyVpcEndpointServicePermissions",
"ec2:ModifyVpcPeeringConnectionOptions",
"ec2:ModifyVpcTenancy",
"ec2:MoveAddressToVpc",
"ec2:RejectVpcEndpointConnections",
"ec2:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceNetworkAclEntry",
"ec2:ReplaceRoute",
"ec2:ReplaceRouteTableAssociation",
"ec2:ResetNetworkInterfaceAttribute",
"ec2:RestoreAddressToClassic",
"ec2:UnassignIpv6Addresses",
"ec2:UnassignPrivateIpAddresses",
"ec2:UpdateSecurityGroupRuleDescriptionsEgress",
"ec2:UpdateSecurityGroupRuleDescriptionsIngress",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
```

```

    "elasticbeanstalk:RequestEnvironmentInfo",
    "elasticbeanstalk:RetrieveEnvironmentInfo",
    "elasticloadbalancing:*",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "route53:*",
    "route53domains:*",
    "sns:CreateTopic",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AcceptVpcPeeringConnection",
    "ec2:AttachClassicLinkVpc",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateVpcPeeringConnection",
    "ec2>DeleteCustomerGateway",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteNetworkAcl",
    "ec2>DeleteNetworkAclEntry",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteVolume",
    "ec2>DeleteVpcPeeringConnection",
    "ec2:DetachClassicLinkVpc",
    "ec2:DisableVpcClassicLink",
    "ec2:EnableVpcClassicLink",
    "ec2:GetConsoleScreenshot",
    "ec2:RejectVpcPeeringConnection",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : [
    "*"
  ]
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLocalGatewayRoute",
    "ec2:CreateLocalGatewayRouteTableVpcAssociation",
    "ec2>DeleteLocalGatewayRoute",
    "ec2>DeleteLocalGatewayRouteTableVpcAssociation",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeLocalGateways",
    "ec2:SearchLocalGatewayRoutes"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "s3:ListBucket"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/flow-logs-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "networkmanager:*"
  ],
  "Resource" : "*"
},
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AcceptTransitGatewayVpcAttachment",
    "ec2:AssociateTransitGatewayRouteTable",
    "ec2:CreateTransitGateway",
    "ec2:CreateTransitGatewayRoute",
    "ec2:CreateTransitGatewayRouteTable",
    "ec2:CreateTransitGatewayVpcAttachment",
    "ec2>DeleteTransitGateway",
    "ec2>DeleteTransitGatewayRoute",
    "ec2>DeleteTransitGatewayRouteTable",
    "ec2>DeleteTransitGatewayVpcAttachment",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DisableTransitGatewayRouteTablePropagation",
    "ec2:DisassociateTransitGatewayRouteTable",
    "ec2:EnableTransitGatewayRouteTablePropagation",
    "ec2:ExportTransitGatewayRoutes",
    "ec2:GetTransitGatewayAttachmentPropagations",
    "ec2:GetTransitGatewayRouteTableAssociations",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:ModifyTransitGateway",
    "ec2:ModifyTransitGatewayVpcAttachment",
    "ec2:RejectTransitGatewayVpcAttachment",
    "ec2:ReplaceTransitGatewayRoute",
    "ec2:SearchTransitGatewayRoutes"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "transitgateway.amazonaws.com"
      ]
    }
  }
}
```

```
    }  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

OAMFullAccess

OAMFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet à CloudWatch Observability Access Manager

Utilisation de cette stratégie

Vous pouvez OAMFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2022, 13:38 UTC
- Heure modifiée : 27 novembre 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

OAMReadOnlyAccess

OAMReadOnlyAccess est une [politiqueAWS gérée](#) qui : Fournit un accès en lecture seule à CloudWatch Observability Access Manager

Utilisation de cette stratégie

Vous pouvez les associer OAMReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 27 novembre 2022, 13:29 UTC
- Heure modifiée : 27 novembre 2022, 13:29 UTC
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

PartnerCentralAccountManagementUserRoleAssociation

PartnerCentralAccountManagementUserRoleAssociation est une [politique AWS gérée](#) qui : fournit un accès permettant d'associer et de dissocier les utilisateurs de Partner Central aux rôles IAM

Utilisation de cette politique

Vous pouvez vous associer `PartnerCentralAccountManagementUserRoleAssociation` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2023, 02:03 UTC
- Heure modifiée : 10 novembre 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
  ],
}
```

```
"Sid" : "PartnerUserRoleAssociation",
"Effect" : "Allow",
"Action" : [
  "iam:ListRoles",
  "partnercentral-account-management:AssociatePartnerUser",
  "partnercentral-account-management:DisassociatePartnerUser"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

PowerUserAccess

PowerUserAccess est une [politique AWS gérée](#) qui : fournit un accès complet aux AWS services et aux ressources, mais n'autorise pas la gestion des utilisateurs et des groupes.

Utilisation de cette politique

Vous pouvez l'associer PowerUserAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 6 juillet 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole",
        "iam>DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeOrganization",
        "account:ListRegions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

QuickSightAccessForS3StorageManagementAnalyticsReadOnly est une [politique AWS gérée](#) qui : Politique utilisée par QuickSight l'équipe pour accéder aux données clients produites par S3 Storage Management Analytics.

Utilisation de cette stratégie

Vous pouvez QuickSightAccessForS3StorageManagementAnalyticsReadOnly les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 12 juin 2017, 18:18 UTC
- Heure modifiée : 8 octobre 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
    "arn:aws:s3:::s3-analytics-export-shared-*"
  ],
},
{
  "Action" : [
    "s3:GetAnalyticsConfiguration",
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

RDSCloudHsmAuthorizationRole

RDSCloudHsmAuthorizationRole est une [politique AWS gérée](#) qui : [Politique](#) par défaut pour le rôle de service Amazon RDS.

Utilisation de cette stratégie

Vous pouvez RDSCloudHsmAuthorizationRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 26 septembre 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ReadOnlyAccess

ReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule aux AWS services et aux ressources.

Utilisation de cette politique

Vous pouvez vous associer ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:39 UTC
- Heure modifiée : 5 février 2024, 15h00 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Version de la politique

Version de la politique : v111 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",

```

```
"access-analyzer:GetFinding",
"access-analyzer:GetGeneratedPolicy",
"access-analyzer:ListAccessPreviewFindings",
"access-analyzer:ListAccessPreviews",
"access-analyzer:ListAnalyzedResources",
"access-analyzer:ListAnalyzers",
"access-analyzer:ListArchiveRules",
"access-analyzer:ListFindings",
"access-analyzer:ListPolicyGenerations",
"access-analyzer:ListTagsForResource",
"access-analyzer:ValidatePolicy",
"account:GetAccountInformation",
"account:GetAlternateContact",
"account:GetChallengeQuestions",
"account:GetContactInformation",
"account:GetRegionOptStatus",
"account:ListRegions",
"acm-pca:Describe*",
"acm-pca:Get*",
"acm-pca:List*",
"acm:Describe*",
"acm:Get*",
"acm:List*",
"airflow:ListEnvironments",
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:GetDomainAssociation",
"amplify:GetJob",
"amplify:ListApps",
"amplify:ListBranches",
"amplify:ListDomainAssociations",
"amplify:ListJobs",
"aoss:BatchGetCollection",
"aoss:BatchGetVpcEndpoint",
"aoss:GetAccessPolicy",
"aoss:GetAccountSettings",
"aoss:GetPoliciesStats",
"aoss:GetSecurityConfig",
"aoss:GetSecurityPolicy",
"aoss:ListAccessPolicies",
"aoss:ListCollections",
"aoss:ListSecurityConfigs",
"aoss:ListSecurityPolicies",
```



```
"aoss:ListTagsForResource",
"aoss:ListVpcEndpoints",
"apigateway:GET",
"appconfig:GetApplication",
"appconfig:GetConfiguration",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appfabric:GetAppAuthorization",
"appfabric:GetAppBundle",
"appfabric:GetIngestion",
"appfabric:GetIngestionDestination",
"appfabric:ListAppAuthorizations",
"appfabric:ListAppBundles",
"appfabric:ListIngestionDestinations",
"appfabric:ListIngestions",
"appfabric:ListTagsForResource",
"appflow:DescribeConnector",
"appflow:DescribeConnectorEntity",
"appflow:DescribeConnectorFields",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeConnectors",
"appflow:DescribeFlow",
"appflow:DescribeFlowExecution",
"appflow:DescribeFlowExecutionRecords",
"appflow:DescribeFlows",
"appflow:ListConnectorEntities",
"appflow:ListConnectorFields",
"appflow:ListConnectors",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:Describe*",
"application-autoscaling:ListTagsForResource",
"applicationinsights:Describe*",
"applicationinsights:List*",
```

```
"appmesh:Describe*",
"appmesh:List*",
"apprunner:DescribeAutoScalingConfiguration",
"apprunner:DescribeCustomDomains",
"apprunner:DescribeObservabilityConfiguration",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:DescribeVpcIngressConnection",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appstream:Describe*",
"appstream:List*",
"appsync:Get*",
"appsync:List*",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"aps:DescribeRuleGroupsNamespace",
"aps:DescribeWorkspace",
"aps:GetAlertManagerSilence",
"aps:GetAlertManagerStatus",
"aps:GetLabels",
"aps:GetMetricMetadata",
"aps:GetSeries",
"aps:ListAlertManagerAlertGroups",
"aps:ListAlertManagerAlerts",
"aps:ListAlertManagerReceivers",
"aps:ListAlertManagerSilences",
"aps:ListAlerts",
"aps:ListRuleGroupsNamespaces",
"aps:ListRules",
"aps:ListTagsForResource",
"aps:ListWorkspaces",
"aps:QueryMetrics",
"arc-zonal-shift:GetManagedResource",
"arc-zonal-shift:ListAutoshifts",
"arc-zonal-shift:ListManagedResources",
"arc-zonal-shift:ListZonalShifts",
"artifact:GetReport",
```

```
"artifact:GetReportMetadata",
"artifact:GetTermForReport",
"artifact:ListReports",
"athena:Batch*",
"athena:Get*",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:GetAssessmentFramework",
"auditmanager:GetAssessmentReportUrl",
"auditmanager:GetChangeLogs",
"auditmanager:GetControl",
"auditmanager:GetDelegations",
"auditmanager:GetEvidence",
"auditmanager:GetEvidenceByEvidenceFolder",
"auditmanager:GetEvidenceFolder",
"auditmanager:GetEvidenceFoldersByAssessment",
"auditmanager:GetEvidenceFoldersByAssessmentControl",
"auditmanager:GetOrganizationAdminAccount",
"auditmanager:GetServicesInScope",
"auditmanager:GetSettings",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControls",
"auditmanager:ListKeywordsForDataSource",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"auditmanager:ValidateAssessmentReportIntegrity",
"autoscaling-plans:Describe*",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:Describe*",
"autoscaling:GetPredictiveScalingForecast",
"aws-portal:View*",
"backup-gateway:GetBandwidthRateLimitSchedule",
"backup-gateway:GetGateway",
"backup-gateway:GetHypervisor",
"backup-gateway:GetHypervisorPropertyMappings",
"backup-gateway:GetVirtualMachine",
"backup-gateway:ListGateways",
"backup-gateway:ListHypervisors",
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:Describe*",
```

```
"backup:Get*",
"backup:List*",
"batch:Describe*",
"batch:List*",
"bedrock:GetAgent",
"bedrock:GetAgentActionGroup",
"bedrock:GetAgentAlias",
"bedrock:GetAgentKnowledgeBase",
"bedrock:GetAgentVersion",
"bedrock:GetCustomModel",
"bedrock:GetDataSource",
"bedrock:GetFoundationModel",
"bedrock:GetFoundationModelAvailability",
"bedrock:GetIngestionJob",
"bedrock:GetKnowledgeBase",
"bedrock:GetModelCustomizationJob",
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:GetProvisionedModelThroughput",
"bedrock:GetUseCaseForModelAccess",
"bedrock:ListAgentActionGroups",
"bedrock:ListAgentAliases",
"bedrock:ListAgentKnowledgeBases",
"bedrock:ListAgents",
"bedrock:ListAgentVersions",
"bedrock:ListCustomModels",
"bedrock:ListDataSources",
"bedrock:ListFoundationModelAgreementOffers",
"bedrock:ListFoundationModels",
"bedrock:ListIngestionJobs",
"bedrock:ListKnowledgeBases",
"bedrock:ListModelCustomizationJobs",
"bedrock:ListProvisionedModelThroughputs",
"billing:GetBillingData",
"billing:GetBillingDetails",
"billing:GetBillingNotifications",
"billing:GetBillingPreferences",
"billing:GetContractInformation",
"billing:GetCredits",
"billing:GetIAMAccessPreference",
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"billingconductor:GetBillingGroupCostReport",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroupCostReports",
```

```
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListCustomLineItemVersions",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingPlansAssociatedWithPricingRule",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListResourcesAssociatedToCustomLineItem",
"billingconductor:ListTagsForResource",
"braket:GetDevice",
"braket:GetJob",
"braket:GetQuantumTask",
"braket:SearchDevices",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"budgets:Describe*",
"budgets:View*",
"cassandra:Select",
"ce:DescribeCostCategoryDefinition",
"ce:DescribeNotificationSubscription",
"ce:DescribeReport",
"ce:GetAnomalies",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"ce:GetApproximateUsageRecords",
"ce:GetCostAndUsage",
"ce:GetCostAndUsageWithResources",
"ce:GetCostCategories",
"ce:GetCostForecast",
"ce:GetDimensionValues",
"ce:GetPreferences",
"ce:GetReservationCoverage",
"ce:GetReservationPurchaseRecommendation",
"ce:GetReservationUtilization",
"ce:GetRightsizingRecommendation",
"ce:GetSavingsPlanPurchaseRecommendationDetails",
"ce:GetSavingsPlansCoverage",
"ce:GetSavingsPlansPurchaseRecommendation",
"ce:GetSavingsPlansUtilization",
"ce:GetSavingsPlansUtilizationDetails",
"ce:GetTags",
"ce:GetUsageForecast",
"ce:ListCostAllocationTags",
"ce:ListCostCategoryDefinitions",
```

```
"ce:ListSavingsPlansPurchaseRecommendationGeneration",
"ce:ListTagsForResource",
"chatbot:Describe*",
"chatbot:Get*",
"chatbot:ListMicrosoftTeamsChannelConfigurations",
"chatbot:ListMicrosoftTeamsConfiguredTeams",
"chatbot:ListMicrosoftTeamsUserIdentities",
"chime:Get*",
"chime:List*",
"chime:Retrieve*",
"chime:Search*",
"chime:Validate*",
"cleanrooms:BatchGetCollaborationAnalysisTemplate",
"cleanrooms:BatchGetSchema",
"cleanrooms:GetAnalysisTemplate",
"cleanrooms:GetCollaboration",
"cleanrooms:GetCollaborationAnalysisTemplate",
"cleanrooms:GetConfiguredTable",
"cleanrooms:GetConfiguredTableAnalysisRule",
"cleanrooms:GetConfiguredTableAssociation",
"cleanrooms:GetMembership",
"cleanrooms:GetProtectedQuery",
"cleanrooms:GetSchema",
"cleanrooms:GetSchemaAnalysisRule",
"cleanrooms:ListAnalysisTemplates",
"cleanrooms:ListCollaborationAnalysisTemplates",
"cleanrooms:ListCollaborations",
"cleanrooms:ListConfiguredTableAssociations",
"cleanrooms:ListConfiguredTables",
"cleanrooms:ListMembers",
"cleanrooms:ListMemberships",
"cleanrooms:ListProtectedQueries",
"cleanrooms:ListSchemas",
"cleanrooms:ListTagsForResource",
"cloud9:Describe*",
"cloud9:List*",
"clouddirectory:BatchRead",
"clouddirectory:Get*",
"clouddirectory:List*",
"clouddirectory:LookupPolicy",
"cloudformation:Describe*",
"cloudformation:Detect*",
"cloudformation:Estimate*",
"cloudformation:Get*",
```

```
"cloudformation:List*",
"cloudformation:ValidateTemplate",
"cloudfront-keyvaluestore:Describe*",
"cloudfront-keyvaluestore:Get*",
"cloudfront-keyvaluestore:List*",
"cloudfront:Describe*",
"cloudfront:Get*",
"cloudfront:List*",
"cloudhsm:Describe*",
"cloudhsm:List*",
"cloudsearch:Describe*",
"cloudsearch:List*",
"cloudtrail:Describe*",
"cloudtrail:Get*",
"cloudtrail:List*",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"codeartifact:DescribeDomain",
"codeartifact:DescribePackage",
"codeartifact:DescribePackageVersion",
"codeartifact:DescribeRepository",
"codeartifact:GetAuthorizationToken",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetPackageVersionAsset",
"codeartifact:GetPackageVersionReadme",
"codeartifact:GetRepositoryEndpoint",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersionAssets",
"codeartifact:ListPackageVersionDependencies",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListRepositoriesInDomain",
"codeartifact:ListTagsForResource",
"codeartifact:ReadFromRepository",
"codebuild:BatchGet*",
"codebuild:DescribeCodeCoverages",
"codebuild:DescribeTestCases",
"codebuild:List*",
"codecatalyst:GetBillingAuthorization",
```

```
"codecatalyst:GetConnection",
"codecatalyst:GetPendingConnection",
"codecatalyst:ListConnections",
"codecatalyst:ListIamRolesForConnection",
"codecatalyst:ListTagsForResource",
"codecommit:BatchGet*",
"codecommit:Describe*",
"codecommit:Get*",
"codecommit:GitPull",
"codecommit:List*",
"codedeploy:BatchGet*",
"codedeploy:Get*",
"codedeploy:List*",
"codeguru-profiler:Describe*",
"codeguru-profiler:Get*",
"codeguru-profiler:List*",
"codeguru-reviewer:Describe*",
"codeguru-reviewer:Get*",
"codeguru-reviewer:List*",
"codepipeline:Get*",
"codepipeline:List*",
"codestar-connections:GetConnection",
"codestar-connections:GetHost",
"codestar-connections:GetRepositoryLink",
"codestar-connections:GetRepositorySyncStatus",
"codestar-connections:GetResourceSyncStatus",
"codestar-connections:GetSyncConfiguration",
"codestar-connections:ListConnections",
"codestar-connections:ListHosts",
"codestar-connections:ListRepositoryLinks",
"codestar-connections:ListRepositorySyncDefinitions",
"codestar-connections:ListSyncConfigurations",
"codestar-connections:ListTagsForResource",
"codestar-notifications:describeNotificationRule",
"codestar-notifications:listEventTypes",
"codestar-notifications:listNotificationRules",
"codestar-notifications:listTagsForResource",
"codestar-notifications:ListTargets",
"codestar:Describe*",
"codestar:Get*",
"codestar:List*",
"codestar:Verify*",
"cognito-identity:Describe*",
"cognito-identity:GetCredentialsForIdentity",
```



```
"cognito-identity:GetIdentityPoolAnalytics",
"cognito-identity:GetIdentityPoolDailyAnalytics",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetIdentityProviderDailyAnalytics",
"cognito-identity:GetOpenIdToken",
"cognito-identity:GetOpenIdTokenForDeveloperIdentity",
"cognito-identity:List*",
"cognito-identity:Lookup*",
"cognito-idp:AdminGet*",
"cognito-idp:AdminList*",
"cognito-idp:Describe*",
"cognito-idp:Get*",
"cognito-idp:List*",
"cognito-sync:Describe*",
"cognito-sync:Get*",
"cognito-sync:List*",
"cognito-sync:QueryRecords",
"comprehend:BatchDetect*",
"comprehend:Classify*",
"comprehend:Contains*",
"comprehend:Describe*",
"comprehend:Detect*",
"comprehend:List*",
"compute-optimizer:DescribeRecommendationExportJobs",
"compute-optimizer:GetAutoScalingGroupRecommendations",
"compute-optimizer:GetEBSVolumeRecommendations",
"compute-optimizer:GetEC2InstanceRecommendations",
"compute-optimizer:GetEC2RecommendationProjectedMetrics",
"compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
"compute-optimizer:GetECSServiceRecommendations",
"compute-optimizer:GetEffectiveRecommendationPreferences",
"compute-optimizer:GetEnrollmentStatus",
"compute-optimizer:GetEnrollmentStatusesForOrganization",
"compute-optimizer:GetLambdaFunctionRecommendations",
"compute-optimizer:GetLicenseRecommendations",
"compute-optimizer:GetRecommendationPreferences",
"compute-optimizer:GetRecommendationSummaries",
"config:BatchGetAggregateResourceConfig",
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config>SelectAggregateResourceConfig",
```

```
"config:SelectResourceConfig",
"connect:Describe*",
"connect:GetContactAttributes",
"connect:GetCurrentMetricData",
"connect:GetCurrentUserData",
"connect:GetFederationToken",
"connect:GetMetricData",
"connect:GetMetricDataV2",
"connect:GetTaskTemplate",
"connect:GetTrafficDistribution",
"connect:List*",
"consoleapp:GetDeviceIdentity",
"consoleapp:ListDeviceIdentities",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendations",
"cost-optimization-hub:ListRecommendationSummaries",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"customer-verification:GetCustomerVerificationDetails",
"customer-verification:GetCustomerVerificationEligibility",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeJobRun",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobRuns",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"databrew:ListTagsForResource",
"dataexchange:Get*",
"dataexchange:List*",
"datapipeline:Describe*",
```

```
"datapipeline:EvaluateExpression",
"datapipeline:Get*",
"datapipeline:List*",
"datapipeline:QueryObjects",
"datapipeline:Validate*",
"datasync:Describe*",
"datasync:List*",
"dax:BatchGetItem",
"dax:Describe*",
"dax:GetItem",
"dax:ListTags",
"dax:Query",
"dax:Scan",
"deepcomposer:GetComposition",
"deepcomposer:GetModel",
"deepcomposer:GetSampleModel",
"deepcomposer:ListCompositions",
"deepcomposer:ListModels",
"deepcomposer:ListSampleModels",
"deepcomposer:ListTrainingTopics",
"detective:BatchGetGraphMemberDatasources",
"detective:BatchGetMembershipDatasources",
"detective:Get*",
"detective:List*",
"detective:SearchGraph",
"devicefarm:Get*",
"devicefarm:List*",
"devops-guru:DescribeAccountHealth",
"devops-guru:DescribeAccountOverview",
"devops-guru:DescribeAnomaly",
"devops-guru:DescribeEventSourcesConfig",
"devops-guru:DescribeFeedback",
"devops-guru:DescribeInsight",
"devops-guru:DescribeOrganizationHealth",
"devops-guru:DescribeOrganizationOverview",
"devops-guru:DescribeOrganizationResourceCollectionHealth",
"devops-guru:DescribeResourceCollectionHealth",
"devops-guru:DescribeServiceIntegration",
"devops-guru:GetCostEstimation",
"devops-guru:GetResourceCollection",
"devops-guru:ListAnomaliesForInsight",
"devops-guru:ListAnomalousLogGroups",
"devops-guru:ListEvents",
"devops-guru:ListInsights",
```

```
"devops-guru:ListMonitoredResources",
"devops-guru:ListNotificationChannels",
"devops-guru:ListOrganizationInsights",
"devops-guru:ListRecommendations",
"devops-guru:SearchInsights",
"devops-guru:StartCostEstimation",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:Get*",
"discovery:List*",
"dlm:Get*",
"dms:Describe*",
"dms:List*",
"dms:Test*",
"drs:DescribeJobLogItems",
"drs:DescribeJobs",
"drs:DescribeLaunchConfigurationTemplates",
"drs:DescribeRecoveryInstances",
"drs:DescribeRecoverySnapshots",
"drs:DescribeReplicationConfigurationTemplates",
"drs:DescribeSourceNetworks",
"drs:DescribeSourceServers",
"drs:GetFailbackReplicationConfiguration",
"drs:GetLaunchConfiguration",
"drs:GetReplicationConfiguration",
"drs:ListExtensibleSourceServers",
"drs:ListLaunchActions",
"drs:ListStagingAccounts",
"drs:ListTagsForResource",
"ds:Check*",
"ds:Describe*",
"ds:Get*",
"ds:List*",
"ds:Verify*",
"dynamodb:BatchGet*",
"dynamodb:Describe*",
"dynamodb:Get*",
"dynamodb:List*",
"dynamodb: PartiQLSelect",
"dynamodb:Query",
"dynamodb:Scan",
"ec2:Describe*",
"ec2:Get*",
"ec2:ListImagesInRecycleBin",
```

```
"ec2:ListSnapshotsInRecycleBin",
"ec2:SearchLocalGatewayRoutes",
"ec2:SearchTransitGatewayRoutes",
"ec2messages:Get*",
"ecr-public:BatchCheckLayerAvailability",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetAuthorizationToken",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchCheck*",
"ecr:BatchGet*",
"ecr:Describe*",
"ecr:Get*",
"ecr:List*",
"ecs:Describe*",
"ecs:List*",
"eks:Describe*",
"eks:List*",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:Request*",
"elasticbeanstalk:Retrieve*",
"elasticbeanstalk:Validate*",
"elasticfilesystem:Describe*",
"elasticfilesystem:ListTagsForResource",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:List*",
"elasticmapreduce:View*",
"elastictranscoder:List*",
"elastictranscoder:Read*",
```

```
"elemental-appliances-software:Get*",
"elemental-appliances-software:List*",
"emr-containers:DescribeJobRun",
"emr-containers:DescribeManagedEndpoint",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListJobRuns",
"emr-containers:ListManagedEndpoints",
"emr-containers:ListTagsForResource",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:GetDashboardForJobRun",
"emr-serverless:GetJobRun",
"emr-serverless:ListApplications",
"emr-serverless:ListJobRuns",
"emr-serverless:ListTagsForResource",
"es:Describe*",
"es:ESHttpGet",
"es:ESHttpHead",
"es:Get*",
"es:List*",
"events:Describe*",
"events:List*",
"events:Test*",
"evidently:GetExperiment",
"evidently:GetExperimentResults",
"evidently:GetFeature",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegmentReferences",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"evidently:TestSegmentPattern",
"firehose:Describe*",
"firehose:List*",
"fis:GetAction",
"fis:GetExperiment",
"fis:GetExperimentTargetAccountConfiguration",
"fis:GetExperimentTemplate",
"fis:GetTargetAccountConfiguration",
```

```
"fis:GetTargetResourceType",
"fis:ListActions",
"fis:ListExperimentResolvedTargets",
"fis:ListExperiments",
"fis:ListExperimentTargetAccountConfigurations",
"fis:ListExperimentTemplates",
"fis:ListTagsForResource",
"fis:ListTargetAccountConfigurations",
"fis:ListTargetResourceTypes",
"fms:GetAdminAccount",
"fms:GetAppsList",
"fms:GetComplianceDetail",
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:GetProtectionStatus",
"fms:GetProtocolsList",
"fms:GetViolationDetails",
"fms:ListAppsLists",
"fms:ListComplianceStatus",
"fms:ListMemberAccounts",
"fms:ListPolicies",
"fms:ListProtocolsLists",
"fms:ListTagsForResource",
"forecast:DescribeAutoPredictor",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:DescribeDatasetImportJob",
"forecast:DescribeExplainability",
"forecast:DescribeExplainabilityExport",
"forecast:DescribeForecast",
"forecast:DescribeForecastExportJob",
"forecast:DescribeMonitor",
"forecast:DescribePredictor",
"forecast:DescribePredictorBacktestExportJob",
"forecast:DescribeWhatIfAnalysis",
"forecast:DescribeWhatIfForecast",
"forecast:DescribeWhatIfForecastExport",
"forecast:GetAccuracyMetrics",
"forecast:ListDatasetGroups",
"forecast:ListDatasetImportJobs",
"forecast:ListDatasets",
"forecast:ListExplainabilities",
"forecast:ListExplainabilityExports",
"forecast:ListForecastExportJobs",
```

```
"forecast:ListForecasts",
"forecast:ListMonitorEvaluations",
"forecast:ListMonitors",
"forecast:ListPredictorBacktestExportJobs",
"forecast:ListPredictors",
"forecast:ListWhatIfAnalyses",
"forecast:ListWhatIfForecastExports",
"forecast:ListWhatIfForecasts",
"forecast:QueryForecast",
"forecast:QueryWhatIfForecast",
"frauddetector:BatchGetVariable",
"frauddetector:DescribeDetector",
"frauddetector:DescribeModelVersions",
"frauddetector:GetBatchImportJobs",
"frauddetector:GetBatchPredictionJobs",
"frauddetector:GetDeleteEventsByEventTypeStatus",
"frauddetector:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector: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:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListMembers",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"internetmonitor:ListMonitors",
"internetmonitor:ListTagsForResource",
"invoicing:GetInvoiceEmailDeliveryPreferences",
"invoicing:GetInvoicePDF",
"invoicing:ListInvoiceSummaries",
"iot:Describe*",
"iot:Get*",
"iot:List*",
"iot1click:DescribeDevice",
"iot1click:DescribePlacement",
"iot1click:DescribeProject",
"iot1click:GetDeviceMethods",
"iot1click:GetDevicesInPlacement",
"iot1click:ListDeviceEvents",
"iot1click:ListDevices",
"iot1click:ListPlacements",
"iot1click:ListProjects",
"iot1click:ListTagsForResource",
"iotanalytics:Describe*",
"iotanalytics:Get*",
```

```
"iotanalytics:List*",
"iotanalytics:SampleChannelData",
"iotevents:DescribeAlarm",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetector",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:DescribeLoggingOptions",
"iotevents:ListAlarmModels",
"iotevents:ListAlarmModelVersions",
"iotevents:ListAlarms",
"iotevents:ListDetectorModels",
"iotevents:ListDetectorModelVersions",
"iotevents:ListDetectors",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"iotfleethub:DescribeApplication",
"iotfleethub:ListApplications",
"iotfleetwise:GetCampaign",
"iotfleetwise:GetDecoderManifest",
"iotfleetwise:GetFleet",
"iotfleetwise:GetLoggingOptions",
"iotfleetwise:GetModelManifest",
"iotfleetwise:GetRegisterAccountStatus",
"iotfleetwise:GetSignalCatalog",
"iotfleetwise:GetVehicle",
"iotfleetwise:GetVehicleStatus",
"iotfleetwise:ListCampaigns",
"iotfleetwise:ListDecoderManifestNetworkInterfaces",
"iotfleetwise:ListDecoderManifests",
"iotfleetwise:ListDecoderManifestSignals",
"iotfleetwise:ListFleets",
"iotfleetwise:ListFleetsForVehicle",
"iotfleetwise:ListModelManifestNodes",
"iotfleetwise:ListModelManifests",
"iotfleetwise:ListSignalCatalogNodes",
"iotfleetwise:ListSignalCatalogs",
"iotfleetwise:ListTagsForResource",
"iotfleetwise:ListVehicles",
"iotfleetwise:ListVehiclesInFleet",
"iotroborunner:GetDestination",
"iotroborunner:GetSite",
"iotroborunner:GetWorker",
"iotroborunner:GetWorkerFleet",
```

```
"iotroborunner:ListDestinations",
"iotroborunner:ListSites",
"iotroborunner:ListWorkerFleets",
"iotroborunner:ListWorkers",
"iotsitewise:Describe*",
"iotsitewise:Get*",
"iotsitewise:List*",
"iotwireless:GetDestination",
"iotwireless:GetDeviceProfile",
"iotwireless:GetEventConfigurationByResourceTypes",
"iotwireless:GetFuotaTask",
"iotwireless:GetLogLevelsByResourceTypes",
"iotwireless:GetMulticastGroup",
"iotwireless:GetMulticastGroupSession",
"iotwireless:GetNetworkAnalyzerConfiguration",
"iotwireless:GetPartnerAccount",
"iotwireless:GetPosition",
"iotwireless:GetPositionConfiguration",
"iotwireless:GetPositionEstimate",
"iotwireless:GetResourceEventConfiguration",
"iotwireless:GetResourceLogLevel",
"iotwireless:GetResourcePosition",
"iotwireless:GetServiceEndpoint",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessDeviceImportTask",
"iotwireless:GetWirelessDeviceStatistics",
"iotwireless:GetWirelessGateway",
"iotwireless:GetWirelessGatewayCertificate",
"iotwireless:GetWirelessGatewayFirmwareInformation",
"iotwireless:GetWirelessGatewayStatistics",
"iotwireless:GetWirelessGatewayTask",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListDestinations",
"iotwireless:ListDeviceProfiles",
"iotwireless:ListDevicesForWirelessDeviceImportTask",
"iotwireless:ListEventConfigurations",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListMulticastGroupsByFuotaTask",
"iotwireless:ListNetworkAnalyzerConfigurations",
"iotwireless:ListPartnerAccounts",
"iotwireless:ListPositionConfigurations",
"iotwireless:ListQueuedMessages",
```

```
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDeviceImportTasks",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGateways",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:BatchGetChannel",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreams",
"ivs:ListStreamSessions",
"ivs:ListTagsForResource",
"ivschat:GetLoggingConfiguration",
"ivschat:GetRoom",
"ivschat:ListLoggingConfigurations",
"ivschat:ListRooms",
"ivschat:ListTagsForResource",
"kafka:Describe*",
"kafka:DescribeCluster",
"kafka:DescribeClusterOperation",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:Get*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafka:ListClusterOperations",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurationRevisions",
"kafka:ListConfigurations",
"kafka:ListKafkaVersions",
"kafka:ListNodes",
"kafka:ListTagsForResource",
"kafkaconnect:DescribeConnector",
"kafkaconnect:DescribeCustomPlugin",
"kafkaconnect:DescribeWorkerConfiguration",
"kafkaconnect:ListConnectors",
```

```
"kafkaconnect:ListCustomPlugins",
"kafkaconnect:ListWorkerConfigurations",
"kendra:BatchGetDocumentStatus",
"kendra:DescribeDataSource",
"kendra:DescribeExperience",
"kendra:DescribeFaq",
"kendra:DescribeIndex",
"kendra:DescribePrincipalMapping",
"kendra:DescribeQuerySuggestionsBlockList",
"kendra:DescribeQuerySuggestionsConfig",
"kendra:DescribeThesaurus",
"kendra:GetQuerySuggestions",
"kendra:GetSnapshots",
"kendra:ListDataSources",
"kendra:ListDataSourceSyncJobs",
"kendra:ListEntityPersonas",
"kendra:ListExperienceEntities",
"kendra:ListExperiences",
"kendra:ListFaqs",
"kendra:ListGroupsOlderThanOrderingId",
"kendra:ListIndices",
"kendra:ListQuerySuggestionsBlockLists",
"kendra:ListTagsForResource",
"kendra:ListThesauri",
"kendra:Query",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kinesisanalytics:Describe*",
"kinesisanalytics:Discover*",
"kinesisanalytics:Get*",
"kinesisanalytics:List*",
"kinesisvideo:Describe*",
"kinesisvideo:Get*",
"kinesisvideo:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lakeformation:DescribeResource",
"lakeformation:GetDataCellsFilter",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetEffectivePermissionsForPath",
"lakeformation:GetLfTag",
"lakeformation:GetResourceLfTags",
```



```
"lakeformation:ListDataCellsFilter",
"lakeformation:ListLfTags",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lakeformation:ListTableStorageOptimizers",
"lakeformation:SearchDatabasesByLfTags",
"lakeformation:SearchTablesByLfTags",
"lambda:Get*",
"lambda:List*",
"launchwizard:DescribeAdditionalNode",
"launchwizard:DescribeProvisionedApp",
"launchwizard:DescribeProvisioningEvents",
"launchwizard:DescribeSettingsSet",
"launchwizard:GetDeployment",
"launchwizard:GetInfrastructureSuggestion",
"launchwizard:GetIpAddress",
"launchwizard:GetResourceCostEstimate",
"launchwizard:GetResourceRecommendation",
"launchwizard:GetSettingsSet",
"launchwizard:GetWorkload",
"launchwizard:GetWorkloadAsset",
"launchwizard:GetWorkloadAssets",
"launchwizard>ListAdditionalNodes",
"launchwizard>ListAllowedResources",
"launchwizard>ListDeploymentEvents",
"launchwizard>ListDeployments",
"launchwizard>ListProvisionedApps",
"launchwizard>ListResourceCostEstimates",
"launchwizard>ListSettingsSets",
"launchwizard>ListWorkloadDeploymentOptions",
"launchwizard>ListWorkloadDeploymentPatterns",
"launchwizard>ListWorkloads",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotChannel",
"lex:DescribeBotLocale",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:Get*",
```

```
"lex:ListBotAliases",
"lex:ListBotChannels",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
"lex:ListBuiltInIntents",
"lex:ListBuiltInSlotTypes",
"lex:ListExports",
"lex:ListImports",
"lex:ListIntents",
"lex:ListSlots",
"lex:ListSlotTypes",
"lex:ListTagsForResource",
"license-manager:Get*",
"license-manager:List*",
"lightsail:GetActiveNames",
"lightsail:GetAlarms",
"lightsail:GetAutoSnapshots",
"lightsail:GetBlueprints",
"lightsail:GetBucketAccessKeys",
"lightsail:GetBucketBundles",
"lightsail:GetBucketMetricData",
"lightsail:GetBuckets",
"lightsail:GetBundles",
"lightsail:GetCertificates",
"lightsail:GetCloudFormationStackRecords",
"lightsail:GetContainerAPIMetadata",
"lightsail:GetContainerImages",
"lightsail:GetContainerServiceDeployments",
"lightsail:GetContainerServiceMetricData",
"lightsail:GetContainerServicePowers",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshot",
"lightsail:GetDiskSnapshots",
"lightsail:GetDistributionBundles",
"lightsail:GetDistributionLatestCacheReset",
"lightsail:GetDistributionMetricData",
"lightsail:GetDistributions",
"lightsail:GetDomain",
"lightsail:GetDomains",
"lightsail:GetExportSnapshotRecords",
"lightsail:GetInstance",
```

```
"lightsail:GetInstanceMetricData",
"lightsail:GetInstancePortStates",
"lightsail:GetInstances",
"lightsail:GetInstanceSnapshot",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstanceState",
"lightsail:GetKeyPair",
"lightsail:GetKeyPairs",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancerMetricData",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetOperation",
"lightsail:GetOperations",
"lightsail:GetOperationsForResource",
"lightsail:GetRegions",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseBlueprints",
"lightsail:GetRelationalDatabaseBundles",
"lightsail:GetRelationalDatabaseEvents",
"lightsail:GetRelationalDatabaseLogEvents",
"lightsail:GetRelationalDatabaseLogStreams",
"lightsail:GetRelationalDatabaseMetricData",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetRelationalDatabaseSnapshot",
"lightsail:GetRelationalDatabaseSnapshots",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"lightsail:Is*",
"logs:Describe*",
"logs:FilterLogEvents",
"logs:Get*",
"logs:ListAnomalies",
"logs:ListLogAnomalyDetectors",
"logs:ListLogDeliveries",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"logs:StartLiveTail",
"logs:StartQuery",
"logs:StopLiveTail",
"logs:StopQuery",
"logs:TestMetricFilter",
"lookoutequipment:DescribeDataIngestionJob",
```

```
"lookoutequipment:DescribeDataset",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:DescribeLabel",
"lookoutequipment:DescribeLabelGroup",
"lookoutequipment:DescribeModel",
"lookoutequipment:DescribeModelVersion",
"lookoutequipment:DescribeResourcePolicy",
"lookoutequipment:DescribeRetrainingScheduler",
"lookoutequipment:ListDataIngestionJobs",
"lookoutequipment:ListDatasets",
"lookoutequipment:ListInferenceEvents",
"lookoutequipment:ListInferenceExecutions",
"lookoutequipment:ListInferenceSchedulers",
"lookoutequipment:ListLabelGroups",
"lookoutequipment:ListLabels",
"lookoutequipment:ListModels",
"lookoutequipment:ListModelVersions",
"lookoutequipment:ListRetrainingSchedulers",
"lookoutequipment:ListSensorStatistics",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:Describe*",
"lookoutmetrics:Get*",
"lookoutmetrics:List*",
"lookoutvision:DescribeDataset",
"lookoutvision:DescribeModel",
"lookoutvision:DescribeModelPackagingJob",
"lookoutvision:DescribeProject",
"lookoutvision:ListDatasetEntries",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"lookoutvision:ListTagsForResource",
"m2:GetApplication",
"m2:GetApplicationVersion",
"m2:GetBatchJobExecution",
"m2:GetDataSetDetails",
"m2:GetDataSetImportTask",
"m2:GetDeployment",
"m2:GetEnvironment",
"m2:ListApplications",
"m2:ListApplicationVersions",
"m2:ListBatchJobDefinitions",
"m2:ListBatchJobExecutions",
"m2:ListDataSetImportHistory",
```

```
"m2:ListDataSets",
"m2:ListDeployments",
"m2:ListEngineVersions",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"machinelearning:Describe*",
"machinelearning:Get*",
"macie2:BatchGetCustomDataIdentifiers",
"macie2:DescribeBuckets",
"macie2:DescribeClassificationJob",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAdministratorAccount",
"macie2:GetAllowList",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetBucketStatistics",
"macie2:GetClassificationExportConfiguration",
"macie2:GetClassificationScope",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindings",
"macie2:GetFindingsFilter",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetFindingStatistics",
"macie2:GetInvitationsCount",
"macie2:GetMacieSession",
"macie2:GetMember",
"macie2:GetResourceProfile",
"macie2:GetRevealConfiguration",
"macie2:GetSensitiveDataOccurrencesAvailability",
"macie2:GetSensitivityInspectionTemplate",
"macie2:GetUsageStatistics",
"macie2:GetUsageTotals",
"macie2:ListAllowLists",
"macie2:ListClassificationJobs",
"macie2:ListClassificationScopes",
"macie2:ListCustomDataIdentifiers",
"macie2:ListFindings",
"macie2:ListFindingsFilters",
"macie2:ListInvitations",
"macie2:ListMembers",
"macie2:ListOrganizationAdminAccounts",
"macie2:ListResourceProfileArtifacts",
"macie2:ListResourceProfileDetections",
"macie2:ListSensitivityInspectionTemplates",
"macie2:ListTagsForResource",
```

```
"macie2:SearchResources",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:GetProposal",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNetworks",
"managedblockchain:ListNodes",
"managedblockchain:ListProposals",
"managedblockchain:ListProposalVotes",
"managedblockchain:ListTagsForResource",
"mediaconnect:DescribeFlow",
"mediaconnect:DescribeOffering",
"mediaconnect:DescribeReservation",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mediaconnect:ListTagsForResource",
"mediaconvert:DescribeEndpoints",
"mediaconvert:Get*",
"mediaconvert:List*",
"medialive:DescribeChannel",
"medialive:DescribeInput",
"medialive:DescribeInputDevice",
"medialive:DescribeInputDeviceThumbnail",
"medialive:DescribeInputSecurityGroup",
"medialive:DescribeMultiplex",
"medialive:DescribeMultiplexProgram",
"medialive:DescribeOffering",
"medialive:DescribeReservation",
"medialive:DescribeSchedule",
"medialive:ListChannels",
"medialive:ListInputDevices",
"medialive:ListInputDeviceTransfers",
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"medialive:ListTagsForResource",
"mediapackage-vod:Describe*",
```

```
"mediapackage-vod:List*",
"mediapackage:Describe*",
"mediapackage:List*",
"mediapackagev2:GetChannel",
"mediapackagev2:GetChannelGroup",
"mediapackagev2:GetChannelPolicy",
"mediapackagev2:GetHeadObject",
"mediapackagev2:GetObject",
"mediapackagev2:GetOriginEndpoint",
"mediapackagev2:GetOriginEndpointPolicy",
"mediapackagev2:ListChannelGroups",
"mediapackagev2:ListChannels",
"mediapackagev2:ListOriginEndpoints",
"mediapackagev2:ListTagsForResource",
"mediastore:DescribeContainer",
"mediastore:DescribeObject",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:GetLifecyclePolicy",
"mediastore:GetMetricPolicy",
"mediastore:GetObject",
"mediastore:ListContainers",
"mediastore:ListItems",
"mediastore:ListTagsForResource",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:ListTags",
"mgh:Describe*",
"mgh:GetHomeRegion",
"mgh:List*",
"mgn:DescribeJobLogItems",
"mgn:DescribeJobs",
"mgn:DescribeLaunchConfigurationTemplates",
"mgn:DescribeReplicationConfigurationTemplates",
"mgn:DescribeSourceServers",
"mgn:DescribeVcenterClients",
"mgn:GetLaunchConfiguration",
"mgn:GetReplicationConfiguration",
"mgn:ListApplications",
"mgn:ListSourceServerActions",
"mgn:ListTemplateActions",
"mgn:ListWaves",
"mobileanalytics:Get*",
```

```
"mobiletargeting:Get*",
"mobiletargeting:List*",
"monitron:GetProject",
"monitron:GetProjectAdminUser",
"monitron:ListProjects",
"monitron:ListTagsForResource",
"mq:Describe*",
"mq:List*",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:DescribeRuleGroupMetadata",
"network-firewall:DescribeTLSInspectionConfiguration",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"network-firewall:ListTagsForResource",
"network-firewall:ListTLSInspectionConfigurations",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectAttachment",
"networkmanager:GetConnections",
"networkmanager:GetConnectPeer",
"networkmanager:GetConnectPeerAssociations",
"networkmanager:GetCoreNetwork",
"networkmanager:GetCoreNetworkChangeEvents",
"networkmanager:GetCoreNetworkChangeSet",
"networkmanager:GetCoreNetworkPolicy",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetNetworkResourceCounts",
"networkmanager:GetNetworkResourceRelationships",
"networkmanager:GetNetworkResources",
"networkmanager:GetNetworkRoutes",
"networkmanager:GetNetworkTelemetry",
"networkmanager:GetResourcePolicy",
"networkmanager:GetRouteAnalysis",
"networkmanager:GetSites",
"networkmanager:GetSiteToSiteVpnAttachment",
"networkmanager:GetTransitGatewayConnectPeerAssociations",
"networkmanager:GetTransitGatewayPeering",
```



```
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:GetTransitGatewayRouteTableAttachment",
"networkmanager:GetVpcAttachment",
"networkmanager:ListAttachments",
"networkmanager:ListConnectPeers",
"networkmanager:ListCoreNetworkPolicyVersions",
"networkmanager:ListCoreNetworks",
"networkmanager:ListPeerings",
"networkmanager:ListTagsForResource",
"nimble:GetEula",
"nimble:GetFeatureMap",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetLaunchProfileInitialization",
"nimble:GetLaunchProfileMember",
"nimble:GetStreamingImage",
"nimble:GetStreamingSession",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:GetStudioMember",
"nimble:ListEulaAcceptances",
"nimble:ListEulas",
"nimble:ListLaunchProfileMembers",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStreamingSessions",
"nimble:ListStudioComponents",
"nimble:ListStudioMembers",
"nimble:ListStudios",
"nimble:ListTagsForResource",
"notifications-contacts:GetEmailContact",
"notifications-contacts:ListEmailContacts",
"notifications-contacts:ListTagsForResource",
"notifications:GetEventRule",
"notifications:GetNotificationConfiguration",
"notifications:GetNotificationEvent",
"notifications:ListChannels",
"notifications:ListEventRules",
"notifications:ListNotificationConfigurations",
"notifications:ListNotificationEvents",
"notifications:ListNotificationHubs",
"notifications:ListTagsForResource",
"oam:GetLink",
"oam:GetSink",
```

```
"oam:GetSinkPolicy",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"omics:Get*",
"omics:List*",
"one:GetDeviceConfigurationTemplate",
"one:GetDeviceInstance",
"one:GetDeviceInstanceConfiguration",
"one:GetSite",
"one:GetSiteAddress",
"one:ListDeviceConfigurationTemplates",
"one:ListDeviceInstances",
"one:ListSites",
"one:ListUsers",
"opsworks-cm:Describe*",
"opsworks-cm:List*",
"opsworks:Describe*",
"opsworks:Get*",
"organizations:Describe*",
"organizations:List*",
"osis:GetPipeline",
"osis:GetPipelineBlueprint",
"osis:GetPipelineChangeProgress",
"osis:ListPipelineBlueprints",
"osis:ListPipelines",
"osis:ListTagsForResource",
"outposts:Get*",
"outposts:List*",
"payment-cryptography:GetAlias",
"payment-cryptography:GetKey",
"payment-cryptography:GetPublicKeyCertificate",
"payment-cryptography:ListAliases",
"payment-cryptography:ListKeys",
"payment-cryptography:ListTagsForResource",
"payments:GetPaymentInstrument",
"payments:GetPaymentStatus",
"payments:ListPaymentPreferences",
"pca-connector-ad:GetConnector",
"pca-connector-ad:GetDirectoryRegistration",
"pca-connector-ad:GetServicePrincipalName",
"pca-connector-ad:GetTemplate",
"pca-connector-ad:GetTemplateGroupAccessControlEntry",
"pca-connector-ad:ListConnectors",
```

```
"pca-connector-ad:ListDirectoryRegistrations",
"pca-connector-ad:ListServicePrincipalNames",
"pca-connector-ad:ListTagsForResource",
"pca-connector-ad:ListTemplateGroupAccessControlEntries",
"pca-connector-ad:ListTemplates",
"personalize:Describe*",
"personalize:Get*",
"personalize:List*",
"pi:DescribeDimensionKeys",
"pi:GetDimensionKeyDetails",
"pi:GetResourceMetadata",
"pi:GetResourceMetrics",
"pi:ListAvailableResourceDimensions",
"pi:ListAvailableResourceMetrics",
"pipes:DescribePipe",
"pipes:ListPipes",
"pipes:ListTagsForResource",
"polly:Describe*",
"polly:Get*",
"polly:List*",
"polly:SynthesizeSpeech",
"pricing:DescribeServices",
"pricing:GetAttributeValues",
"pricing:GetPriceListFileUrl",
"pricing:GetProducts",
"pricing:ListPriceLists",
"proton:GetDeployment",
"proton:GetEnvironment",
"proton:GetEnvironmentTemplate",
"proton:GetEnvironmentTemplateVersion",
"proton:GetService",
"proton:GetServiceInstance",
"proton:GetServiceTemplate",
"proton:GetServiceTemplateVersion",
"proton:ListDeployments",
"proton:ListEnvironmentAccountConnections",
"proton:ListEnvironments",
"proton:ListEnvironmentTemplates",
"proton:ListServiceInstances",
"proton:ListServices",
"proton:ListServiceTemplates",
"proton:ListTagsForResource",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:ListPurchaseOrderInvoices",
```

```
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ViewPurchaseOrders",
"qldb:DescribeJournalKinesisStream",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:GetBlock",
"qldb:GetDigest",
"qldb:GetRevision",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"qldb:ListTagsForResource",
"ram:Get*",
"ram:List*",
"rbin:GetRule",
"rbin:ListRules",
"rbin:ListTagsForResource",
"rds:Describe*",
"rds:Download*",
"rds:List*",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"redshift:View*",
"refactor-spaces:GetApplication",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetResourcePolicy",
"refactor-spaces:GetRoute",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListEnvironmentVpcs",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"refactor-spaces:ListTagsForResource",
"rekognition:CompareFaces",
"rekognition:DescribeDataset",
"rekognition:DescribeProjects",
"rekognition:DescribeProjectVersions",
"rekognition:DescribeStreamProcessor",
"rekognition:Detect*",
"rekognition:GetCelebrityInfo",
"rekognition:GetCelebrityRecognition",
"rekognition:GetContentModeration",
```

```
"rekognition:GetFaceDetection",
"rekognition:GetFaceSearch",
"rekognition:GetLabelDetection",
"rekognition:GetPersonTracking",
"rekognition:GetSegmentDetection",
"rekognition:GetTextDetection",
"rekognition:List*",
"rekognition:RecognizeCelebrities",
"rekognition:Search*",
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppAssessment",
"resiliencehub:DescribeAppVersion",
"resiliencehub:DescribeAppVersionAppComponent",
"resiliencehub:DescribeAppVersionResource",
"resiliencehub:DescribeAppVersionResourcesResolutionStatus",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListAlarmRecommendations",
"resiliencehub:ListAppAssessmentComplianceDrifts",
"resiliencehub:ListAppAssessments",
"resiliencehub:ListAppComponentCompliances",
"resiliencehub:ListAppComponentRecommendations",
"resiliencehub:ListAppInputSources",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionAppComponents",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListAppVersionResources",
"resiliencehub:ListAppVersions",
"resiliencehub:ListRecommendationTemplates",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListSopRecommendations",
"resiliencehub:ListSuggestedResiliencyPolicies",
"resiliencehub:ListTagsForResource",
"resiliencehub:ListTestRecommendations",
"resiliencehub:ListUnsupportedAppVersionResources",
"resource-explorer-2:BatchGetView",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:GetView",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
```

```
"resource-explorer-2:Search",
"resource-groups:Get*",
"resource-groups:List*",
"resource-groups:Search*",
"robomaker:BatchDescribe*",
"robomaker:Describe*",
"robomaker:Get*",
"robomaker:List*",
"route53-recovery-cluster:Get*",
"route53-recovery-cluster:ListRoutingControls",
"route53-recovery-control-config:Describe*",
"route53-recovery-control-config:GetResourcePolicy",
"route53-recovery-control-config:List*",
"route53-recovery-readiness:Get*",
"route53-recovery-readiness:List*",
"route53:Get*",
"route53:List*",
"route53:Test*",
"route53domains:Check*",
"route53domains:Get*",
"route53domains:List*",
"route53domains:View*",
"route53resolver:Get*",
"route53resolver:List*",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"s3-object-lambda:GetObject",
"s3-object-lambda:GetObjectAcl",
"s3-object-lambda:GetObjectLegalHold",
"s3-object-lambda:GetObjectRetention",
"s3-object-lambda:GetObjectTagging",
"s3-object-lambda:GetObjectVersion",
"s3-object-lambda:GetObjectVersionAcl",
"s3-object-lambda:GetObjectVersionTagging",
"s3-object-lambda:ListBucket",
"s3-object-lambda:ListBucketMultipartUploads",
"s3-object-lambda:ListBucketVersions",
"s3-object-lambda:ListMultipartUploadParts",
"s3:DescribeJob",
"s3:Get*",
"s3:List*",
"sagemaker-groundtruth-synthetic:GetAccountDetails",
"sagemaker-groundtruth-synthetic:GetBatch",
```

```
"sagemaker-groundtruth-synthetic:GetProject",
"sagemaker-groundtruth-synthetic>ListBatchDataTransfers",
"sagemaker-groundtruth-synthetic>ListBatchSummaries",
"sagemaker-groundtruth-synthetic>ListProjectDataTransfers",
"sagemaker-groundtruth-synthetic>ListProjectSummaries",
"sagemaker:Describe*",
"sagemaker:GetSearchSuggestions",
"sagemaker:List*",
"sagemaker:Search",
"savingsplans:DescribeSavingsPlanRates",
"savingsplans:DescribeSavingsPlans",
"savingsplans:DescribeSavingsPlansOfferingRates",
"savingsplans:DescribeSavingsPlansOfferings",
"savingsplans:ListTagsForResource",
"scheduler:GetSchedule",
"scheduler:GetScheduleGroup",
"scheduler>ListScheduleGroups",
"scheduler>ListSchedules",
"scheduler>ListTagsForResource",
"schemas:Describe*",
"schemas:Get*",
"schemas>List*",
"schemas:Search*",
"sdb:Get*",
"sdb>List*",
"sdb>Select*",
"secretsmanager:Describe*",
"secretsmanager:GetResourcePolicy",
"secretsmanager>List*",
"securityhub:BatchGetControlEvaluations",
"securityhub:BatchGetSecurityControls",
"securityhub:BatchGetStandardsControlAssociations",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub>List*",
"serverlessrepo:Get*",
"serverlessrepo>List*",
"serverlessrepo:SearchApplications",
"servicecatalog:Describe*",
"servicecatalog:GetApplication",
"servicecatalog:GetAttributeGroup",
"servicecatalog>List*",
"servicecatalog:Scan*",
"servicecatalog:Search*",
```

```
"servicediscovery:DiscoverInstances",
"servicediscovery:DiscoverInstancesRevision",
"servicediscovery:Get*",
"servicediscovery:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"ses:BatchGetMetricData",
"ses:Describe*",
"ses:Get*",
"ses:List*",
"shield:Describe*",
"shield:Get*",
"shield:List*",
"signer:DescribeSigningJob",
"signer:GetSigningPlatform",
"signer:GetSigningProfile",
"signer:ListProfilePermissions",
"signer:ListSigningJobs",
"signer:ListSigningPlatforms",
"signer:ListSigningProfiles",
"signer:ListTagsForResource",
"sms-voice:DescribeAccountAttributes",
"sms-voice:DescribeAccountLimits",
"sms-voice:DescribeConfigurationSets",
"sms-voice:DescribeKeywords",
"sms-voice:DescribeOptedOutNumbers",
"sms-voice:DescribeOptOutLists",
"sms-voice:DescribePhoneNumbers",
"sms-voice:DescribePools",
"sms-voice:DescribeSenderId",
"sms-voice:DescribeSpendLimits",
"sms-voice:ListPoolOriginationIdentities",
"sms-voice:ListTagsForResource",
"snowball:Describe*",
"snowball:Get*",
```



```
"snowball:List*",
"sns:Check*",
"sns:Get*",
"sns:List*",
"sqs:Get*",
"sqs:List*",
"sqs:Receive*",
"ssm-contacts:DescribeEngagement",
"ssm-contacts:DescribePage",
"ssm-contacts:GetContact",
"ssm-contacts:GetContactChannel",
"ssm-contacts:ListContactChannels",
"ssm-contacts:ListContacts",
"ssm-contacts:ListEngagements",
"ssm-contacts:ListPageReceipts",
"ssm-contacts:ListPagesByContact",
"ssm-contacts:ListPagesByEngagement",
"ssm-incidents:GetIncidentRecord",
"ssm-incidents:GetReplicationSet",
"ssm-incidents:GetResourcePolicies",
"ssm-incidents:GetResponsePlan",
"ssm-incidents:GetTimelineEvent",
"ssm-incidents:ListIncidentRecords",
"ssm-incidents:ListRelatedItems",
"ssm-incidents:ListReplicationSets",
"ssm-incidents:ListResponsePlans",
"ssm-incidents:ListTagsForResource",
"ssm-incidents:ListTimelineEvents",
"ssm:Describe*",
"ssm:Get*",
"ssm:List*",
"sso-directory:Describe*",
"sso-directory:List*",
"sso-directory:Search*",
"sso:Describe*",
"sso:Get*",
"sso:List*",
"sso:Search*",
"states:Describe*",
"states:GetExecutionHistory",
"states:List*",
"storagegateway:Describe*",
"storagegateway:List*",
"sts:GetAccessKeyInfo",
```

```
"sts:GetCallerIdentity",
"sts:GetSessionToken",
"support:DescribeAttachment",
"support:DescribeCases",
"support:DescribeCommunications",
"support:DescribeServices",
"support:DescribeSeverityLevels",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
"support:DescribeTrustedAdvisorCheckResult",
"support:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"supportplans:GetSupportPlan",
"supportplans:GetSupportPlanUpdateStatus",
"sustainability:GetCarbonFootprintSummary",
"swf:Count*",
"swf:Describe*",
"swf:Get*",
"swf:List*",
"synthetics:Describe*",
"synthetics:Get*",
"synthetics:List*",
>tag:DescribeReportCreation",
>tag:Get*",
"tax:GetExemptions",
"tax:GetTaxInheritance",
"tax:GetTaxInterview",
"tax:GetTaxRegistration",
"tax:GetTaxRegistrationDocument",
"tax:ListTaxRegistrations",
"timestream:DescribeBatchLoadTask",
"timestream:DescribeDatabase",
"timestream:DescribeEndpoints",
"timestream:DescribeTable",
"timestream:ListBatchLoadTasks",
"timestream:ListDatabases",
"timestream:ListMeasures",
"timestream:ListTables",
"timestream:ListTagsForResource",
"tnb:GetSolFunctionInstance",
"tnb:GetSolFunctionPackage",
"tnb:GetSolFunctionPackageContent",
"tnb:GetSolFunctionPackageDescriptor",
"tnb:GetSolNetworkInstance",
"tnb:GetSolNetworkOperation",
```

```
"tnb:GetSolNetworkPackage",
"tnb:GetSolNetworkPackageContent",
"tnb:GetSolNetworkPackageDescriptor",
"tnb:ListSolFunctionInstances",
"tnb:ListSolFunctionPackages",
"tnb:ListSolNetworkInstances",
"tnb:ListSolNetworkOperations",
"tnb:ListSolNetworkPackages",
"tnb:ListTagsForResource",
"transcribe:Get*",
"transcribe:List*",
"transfer:Describe*",
"transfer:List*",
"transfer:TestIdentityProvider",
"translate:DescribeTextTranslationJob",
"translate:GetParallelData",
"translate:GetTerminology",
"translate:ListParallelData",
"translate:ListTerminologies",
"translate:ListTextTranslationJobs",
"trustedadvisor:Describe*",
"verifiedpermissions:GetIdentitySource",
"verifiedpermissions:GetPolicy",
"verifiedpermissions:GetPolicyStore",
"verifiedpermissions:GetPolicyTemplate",
"verifiedpermissions:GetSchema",
"verifiedpermissions:IsAuthorized",
"verifiedpermissions:IsAuthorizedWithToken",
"verifiedpermissions:ListIdentitySources",
"verifiedpermissions:ListPolicies",
"verifiedpermissions:ListPolicyStores",
"verifiedpermissions:ListPolicyTemplates",
"vpc-lattice:GetAccessLogSubscription",
"vpc-lattice:GetAuthPolicy",
"vpc-lattice:GetListener",
"vpc-lattice:GetResourcePolicy",
"vpc-lattice:GetRule",
"vpc-lattice:GetService",
"vpc-lattice:GetServiceNetwork",
"vpc-lattice:GetServiceNetworkServiceAssociation",
"vpc-lattice:GetServiceNetworkVpcAssociation",
"vpc-lattice:GetTargetGroup",
"vpc-lattice:ListAccessLogSubscriptions",
"vpc-lattice:ListListeners",
```

```
"vpc-lattice:ListRules",
"vpc-lattice:ListServiceNetworks",
"vpc-lattice:ListServiceNetworkServiceAssociations",
"vpc-lattice:ListServiceNetworkVpcAssociations",
"vpc-lattice:ListServices",
"vpc-lattice:ListTagsForResource",
"vpc-lattice:ListTargetGroups",
"vpc-lattice:ListTargets",
"waf-regional:Get*",
"waf-regional:List*",
"waf:Get*",
"waf:List*",
"wafv2:CheckCapacity",
"wafv2:Describe*",
"wafv2:Get*",
"wafv2:List*",
"wellarchitected:ExportLens",
"wellarchitected:GetAnswer",
"wellarchitected:GetConsolidatedReport",
"wellarchitected:GetLens",
"wellarchitected:GetLensReview",
"wellarchitected:GetLensReviewReport",
"wellarchitected:GetLensVersionDifference",
"wellarchitected:GetMilestone",
"wellarchitected:GetProfile",
"wellarchitected:GetProfileTemplate",
"wellarchitected:GetReviewTemplate",
"wellarchitected:GetReviewTemplateAnswer",
"wellarchitected:GetReviewTemplateLensReview",
"wellarchitected:GetWorkload",
"wellarchitected:ListAnswers",
"wellarchitected:ListCheckDetails",
"wellarchitected:ListCheckSummaries",
"wellarchitected:ListLenses",
"wellarchitected:ListLensReviewImprovements",
"wellarchitected:ListLensReviews",
"wellarchitected:ListLensShares",
"wellarchitected:ListMilestones",
"wellarchitected:ListNotifications",
"wellarchitected:ListProfileNotifications",
"wellarchitected:ListProfiles",
"wellarchitected:ListProfileShares",
"wellarchitected:ListReviewTemplateAnswers",
"wellarchitected:ListReviewTemplates",
```

```

    "wellarchitected:ListShareInvitations",
    "wellarchitected:ListTagsForResource",
    "wellarchitected:ListTemplateShares",
    "wellarchitected:ListWorkloads",
    "wellarchitected:ListWorkloadShares",
    "workdocs:CheckAlias",
    "workdocs:Describe*",
    "workdocs:Get*",
    "workmail:Describe*",
    "workmail:Get*",
    "workmail:List*",
    "workmail:Search*",
    "workspaces-web:GetBrowserSettings",
    "workspaces-web:GetIdentityProvider",
    "workspaces-web:GetNetworkSettings",
    "workspaces-web:GetPortal",
    "workspaces-web:GetPortalServiceProviderMetadata",
    "workspaces-web:GetTrustStore",
    "workspaces-web:GetUserAccessLoggingSettings",
    "workspaces-web:GetUserSettings",
    "workspaces-web:ListBrowserSettings",
    "workspaces-web:ListIdentityProviders",
    "workspaces-web:ListNetworkSettings",
    "workspaces-web:ListPortals",
    "workspaces-web:ListTagsForResource",
    "workspaces-web:ListTrustStores",
    "workspaces-web:ListUserAccessLoggingSettings",
    "workspaces-web:ListUserSettings",
    "workspaces:Describe*",
    "xray:BatchGet*",
    "xray:Get*"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ResourceGroupsandTagEditorFullAccess

ResourceGroupsandTagEditorFullAccess est un [AWS politique gérée](#) qui : fournit un accès complet aux groupes de ressources et à l'éditeur de balises.

Utilisation de cette politique

Vous pouvez joindre ResourceGroupsandTagEditorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 06 février 2015, 18:39 UTC
- Heure modifiée : 10 août 2023, 13 h 29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à un AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
    "tag:getTagKeys",
    "tag:getTagValues",
    "tag:TagResources",
    "tag:UntagResources",
    "resource-groups:*",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations du moindre privilège](#)

ResourceGroupsandTagEditorReadOnlyAccess

ResourceGroupsandTagEditorReadOnlyAccess est un [AWS politique gérée](#) qui : permet d'utiliser les groupes de ressources et l'éditeur de balises, mais n'autorise pas la modification des balises via l'éditeur de balises.

Utilisation de cette politique

Vous pouvez joindre ResourceGroupsandTagEditorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: AWS politique gérée
- Heure de création: 06 février 2015, 18:39 UTC
- Heure modifiée : 10 août 2023, 13 h 42 UTC

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

Version de la politique

Version de la politique : v3(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à unAWSressource,AWSvérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations du moindre privilège](#)

ResourceGroupsServiceRolePolicy

ResourceGroupsServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise les AWS Resource Groups à interroger les AWS services propriétaires de vos ressources pour conserver le groupe up-to-date

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les rôles attachés à vos rôles, les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 5 janvier 2023, 16:57 UTC
- Heure modifiée : 5 janvier 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations gérées et évoluez vers les autorisations gérées et évoluez vers les autorisations gérées](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy est une [politiqueAWS gérée](#) qui : autorise l'opérateur du pilote OpenShift Amazon EBS Container Storage Interface (CSI) à installer et à gérer le pilote Amazon EBS CSI sur un cluster Red Hat OpenShift Service on AWS (ROSA). Le pilote CSI Amazon EBS permet aux clusters ROSA de gérer le cycle de vie des volumes Amazon EBS pour les volumes persistants.

Utilisation de cette stratégie

Vous pouvez les associer ROSAAmazonEBSCSIDriverOperatorPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2023, 22:36 UTC
- Heure modifiée : 20 avril 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
```

```
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSnapshotResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSnapshotRequestTag",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : [
```

```
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateVolume",
        "CreateSnapshot"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy est une [politiqueAWS gérée](#) qui : Permet à l'opérateur OpenShift Cloud Network Config Controller de provisionner et de gérer des ressources réseau destinées à être utilisées par la superposition réseau du cluster Red Hat OpenShift Service on AWS (ROSA). L'opérateur de réseau OpenShift cloud s'interface avec AWS les API pour le compte des plugins réseau via CustomResourceDefinitions. L'opérateur utilise ces autorisations politiques pour gérer les adresses IP privées des instances Amazon EC2 dans le cadre du cluster ROSA.

Utilisation de cette stratégie

Vous pouvez les associer ROSACloudNetworkConfigOperatorPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2023, 22:34 UTC
- Heure modifiée : 20 avril 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)

- [Démarez avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ROSAControlPlaneOperatorPolicy

ROSAControlPlaneOperatorPolicy est une [politique AWS gérée](#) qui : permet à Red Hat OpenShift Service on AWS (ROSA) Control Plane (ROSA) de gérer les ressources Amazon EC2 et Amazon Route 53 du cluster ROSA.

Utilisation de cette politique

Vous pouvez ROSAControlPlaneOperatorPolicy l'associer à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 avril 2023, 23:02 UTC
- Heure modifiée : 30 juin 2023, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
```



```
    "route53:ListHostedZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DeleteSecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "SecurityGroupIngressEgress",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress"
  ],
  "Resource" : [
```

```
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroupsVPCNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "ListResourceRecordSets",
  "Effect" : "Allow",
  "Action" : [
    "route53:ListResourceRecordSets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
  "Effect" : "Allow",
  "Action" : [
    "route53:ChangeResourceRecordSets"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
        "/*.hypershift.local"
      ]
    }
  }
}
```

```
  },
  {
    "Sid" : "VPCEndpointWithCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "VPCEndpointResourceTagCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "VPCEndpointNoCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*"
    ]
  },
  {
```

```
"Sid" : "ManageVPCEndpointWithCondition",
"Effect" : "Allow",
"Action" : [
  "ec2:ModifyVpcEndpoint",
  "ec2>DeleteVpcEndpoints"
],
"Resource" : [
  "arn:aws:ec2:*:*:vpc-endpoint/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat-managed" : "true"
  }
}
},
{
  "Sid" : "ModifyVPCEndpoingNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*",
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateVpcEndpoint",
        "CreateSecurityGroup"
      ]
    }
  }
}
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

ROSAImageRegistryOperatorPolicy

ROSAImageRegistryOperatorPolicy est une [politique AWS gérée](#) qui : permet à l'opérateur du registre OpenShift d'images de provisionner et de gérer des compartiments et des objets Amazon S3 à utiliser par le registre d'images intégré au cluster Red Hat OpenShift Service on AWS (ROSA) afin de répondre aux exigences de stockage ROSA. L'opérateur de registre d' OpenShift images installe et gère le registre interne d'un OpenShift cluster Red Hat.

Utilisation de cette politique

Vous pouvez vous associer ROSAImageRegistryOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 27 avril 2023, 20:13 UTC
- Heure modifiée : 12 décembre 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3>DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",

```

```
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/**",
    "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ROSAIngressOperatorPolicy

ROSAIngressOperatorPolicy est une [politique AWS gérée](#) qui : Permet à l'opérateur d'OpenShift entrée de configurer et de gérer des équilibres de charge et des configurations de système de noms de domaine (DNS) pour les clusters Red Hat OpenShift Service on AWS (ROSA). La politique autorise l'accès en lecture aux valeurs des balises, que l'opérateur filtre pour les ressources Route 53 afin de découvrir les zones hébergées.

Utilisation de cette stratégie

Vous pouvez ROSAIngressOperatorPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2023, 22:37 UTC
- Heure modifiée : 20 avril 2023, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ROSAInstallerPolicy

ROSAInstallerPolicy est une [politique AWS gérée](#) qui : autorise le programme d'installation de Red Hat OpenShift Service on AWS (ROSA) à gérer les AWS ressources qui prennent en charge l'installation du cluster ROSA. Cela inclut la gestion des profils d'instance pour les nœuds de travail ROSA.

Utilisation de cette politique

Vous pouvez vous associer ROSAInstallerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 06 juin 2023, 21h00 UTC
- Heure modifiée : 26 janvier 2024, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Sid" : "ReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeRegions",
      "ec2:DescribeReservedInstancesOfferings",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeInstanceTypeOfferings",
      "elasticloadbalancing:DescribeAccountLimits",
      "elasticloadbalancing:DescribeLoadBalancers",
      "iam:GetOpenIDConnectProvider",
      "iam:GetRole",
      "route53:GetHostedZone",
      "route53:ListHostedZones",
      "route53:ListHostedZonesByName",
      "route53:ListResourceRecordSets",
      "route53:GetAccountLimit",
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PassRoleToEC2",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:*:iam:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  }
]
```

```
    ]
  }
}
},
{
  "Sid" : "ManageInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:instance-profile/rosa-service-managed-*"
  ]
},
{
  "Sid" : "CreateInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile",
    "iam:TagInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:instance-profile/rosa-service-managed-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "GetSecretValue",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
```

```
        "aws:ResourceTag/red-hat-managed" : "true"
    }
}
},
{
    "Sid" : "Route53ManageRecords",
    "Effect" : "Allow",
    "Action" : [
        "route53:ChangeResourceRecordSets"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringLike" : {
            "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
                "*.openshiftapps.com",
                "*.devshift.org",
                "*.hypershift.local",
                "*.openshiftusgov.com",
                "*.devshiftusgov.com"
            ]
        }
    }
},
{
    "Sid" : "Route53Manage",
    "Effect" : "Allow",
    "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
```

```

    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances"
      ]
    }
  },
  {
    "Sid" : "RunInstancesNoCondition",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:snapshot/*"
    ]
  },
  {
    "Sid" : "RunInstancesRestrictedRequestTag",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "RunInstancesRedHatOwnedAMIs",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:Owner" : [

```

```
        "531415883065",
        "251351625822",
        "210686502322"
    ]
}
},
{
    "Sid" : "ManageInstancesRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "CreateGrantRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
            "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
            "kms:GrantIsForAWSResource" : true
        }
    }
},
{
    "Sid" : "ManagedKMSRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
```

```
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DeleteSecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "SecurityGroupIngressEgress",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroupsVPCNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup"
      ]
    }
  }
}
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ROSAKMSProviderPolicy

ROSAKMSProviderPolicy est une [politique AWS gérée](#) qui : Permet au fournisseur de AWS chiffrement ROSA intégré de gérer les AWS clés du service de gestion des clés (KMS) afin de prendre en charge le chiffrement des données, etc., à l'aide d'une clé AWS KMS fournie par le client. La politique autorise le chiffrement et le déchiffrement des données à l'aide de clés KMS.

Utilisation de cette stratégie

Vous pouvez ROSAKMSProviderPolicy les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 27 avril 2023, 20:10 UTC
- Heure modifiée : 27 avril 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "VolumeEncryption",
    "Effect" : "Allow",
    "Action" : [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat" : "true"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ROSAKubeControllerPolicy

ROSAKubeControllerPolicy est une [politique AWS gérée](#) qui : permet au contrôleur ROSA Kubernetes de gérer les ressources Amazon EC2, Elastic Load Balancing (ELB) et AWS Key Management Service (KMS) pour un cluster ROSA.

Utilisation de cette politique

Vous pouvez vous associer ROSAKubeControllerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service

- Heure de création : 27 avril 2023, 20:09 UTC
- Heure modifiée : 16 octobre 2023, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
```

```
"Action" : [
  "kms:DescribeKey"
],
"Resource" : [
  "*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat" : "true"
  }
}
},
{
  "Sid" : "LoadBalancerManagement",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:ConfigureHealthCheck",
    "elasticloadbalancing:CreateLoadBalancerPolicy",
    "elasticloadbalancing>DeleteLoadBalancer",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:ModifyLoadBalancerAttributes",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "CreateTargetGroup",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
}
},
```

```
{
  "Sid" : "LoadBalancerManagementResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DeleteListener",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:ModifyTargetGroup",
    "elasticloadbalancing>DeleteTargetGroup",
    "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
    "elasticloadbalancing>CreateLoadBalancerListeners",
    "elasticloadbalancing>DeleteLoadBalancerListeners",
    "elasticloadbalancing:AttachLoadBalancerToSubnets",
    "elasticloadbalancing:DetachLoadBalancerFromSubnets",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateListeners",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing>CreateListener"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true",
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroup",
  "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateSecurityGroup"
],
"Resource" : [
  "arn:aws:ec2:*:*:security-group/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/red-hat-managed" : "true"
  }
}
},
{
  "Sid" : "CreateSecurityGroupVpc",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "CreateLoadBalancer",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:CreateLoadBalancer"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
}
},
{
  "Sid" : "ModifySecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup"
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "CreateTagsSecurityGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ROSAManageSubscription

ROSAManageSubscription est un [AWS politique gérée](#) cela : Cette politique fournit les autorisations requises pour gérer le Red Hat OpenShift Service activé AWS Abonnement (ROSA).

Utilisation de cette politique

Vous pouvez joindre `ROSAManageSubscription` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: `AWS` politique gérée
- Heure de création: 11 avril 2022, 20:58 UTC
- Heure modifiée : 4 août 2023, 19h59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Version de la politique

Version de la politique : v2(par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à un `AWS` ressource, `AWS` vérifie la version par défaut de la politique pour déterminer si la demande doit être autorisée.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    }
  ]
}
```



```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide de AWS politiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec AWS politiques gérées et évolution vers les autorisations de moindre privilège](#)

ROSANodePoolManagementPolicy

ROSANodePoolManagementPolicy est une [politique AWS gérée](#) qui : permet à Red Hat OpenShift Service on AWS (ROSA) de gérer les instances EC2 du cluster en tant que nœuds de travail, y compris l'autorisation de configurer des groupes de sécurité et de baliser des instances et des volumes. Cette politique autorise également l'utilisation d'instances EC2 avec un chiffrement de disque fourni par des clés du service de gestion des AWS clés (KMS).

Utilisation de cette stratégie

Vous pouvez l'associer ROSANodePoolManagementPolicy à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : Politique relative aux rôles de service
- Heure de création : 8 juin 2023, 20:48 UTC
- Heure modifiée : 8 juin 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam:*:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
```

```
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
}
},
{
    "Sid" : "PassWorkerRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:*:iam:*:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "ec2.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "NetworkInterfaces",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : [
```

```
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "NetworkInterfacesNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "TerminateInstances",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
}
```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances"
        ]
      }
    }
  },
  {
    "Sid" : "CreateTagsCAPAControllerReconcileInstance",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "CreateTagsCAPAControllerReconcileVolume",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "RunInstancesRequest",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "RunInstancesNoCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*"
    ]
  },
  {
    "Sid" : "RunInstancesRedHatAMI",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:Owner" : [
          "531415883065",
          "251351625822"
        ]
      }
    }
  },
  {
    "Sid" : "ManagedKMSRestrictedResourceTag",
    "Effect" : "Allow",
```

```
"Action" : [
  "kms:DescribeKey",
  "kms:GenerateDataKeyWithoutPlaintext"
],
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/red-hat" : "true"
  }
}
},
{
  "Sid" : "CreateGrantRestricted",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    },
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    }
  }
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ROSASRESupportPolicy

ROSASRESupportPolicy est une [politique AWS gérée](#) qui : fournit à l'ingénierie de fiabilité du site (SRE) de ROSA les autorisations nécessaires pour initialement observer, diagnostiquer et prendre en charge les AWS ressources associées aux clusters Red Hat OpenShift Service on AWS (ROSA), y compris la possibilité de modifier l'état du nœud du cluster ROSA.

Utilisation de cette politique

Vous pouvez vous associer ROSASRESupportPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique des rôles de service
- Heure de création : 01 juin 2023, 14:36 UTC
- Heure modifiée : 22 janvier 2024, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ]
    }
  ],
}
```



```
    "Resource" : "*"
  },
  {
    "Sid" : "Route53",
    "Effect" : "Allow",
    "Action" : [
      "route53:GetHostedZone",
      "route53:GetHostedZoneCount",
      "route53:ListHostedZones",
      "route53:ListHostedZonesByName",
      "route53:ListResourceRecordSets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "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:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "DescribeSpotFleetInstances",
    "Effect" : "Allow",
    "Action" : "ec2:DescribeSpotFleetInstances",
    "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "DescribeVolumeAttribute",
    "Effect" : "Allow",
    "Action" : "ec2:DescribeVolumeAttribute",
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Resource" : "*"
  }
}
```

```
"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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ROSAWorkerInstancePolicy

ROSAWorkerInstancePolicy est une [politique AWS gérée](#) qui : autorise les nœuds de travail Red Hat OpenShift Service on AWS (ROSA) de votre compte à accéder en lecture seule aux instances Amazon EC2 et à la gestion du cycle de vie des nœuds de calcul.

Utilisation de cette stratégie

Vous pouvez associer ROSAWorkerInstancePolicy à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 avril 2023, 22:35 UTC

- Heure modifiée : 20 avril 2023, 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

Route53RecoveryReadinessServiceRolePolicy

Route53RecoveryReadinessServiceRolePolicy est une [politique AWS gérée](#) qui : **Politique** de rôle liée aux services pour Route 53 Recovery Readiness

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à ce service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 15 juillet 2021, 16:06 UTC
- Heure modifiée : 14 février 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Version de la politique

Version de la politique :v5 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DescribeTable",
    "dynamodb:DescribeTimeToLive"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/AWSServiceRoleForServiceQuotas",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "servicequotas.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunctionConcurrency",
    "lambda:GetFunctionConfiguration",
    "lambda:GetProvisionedConcurrencyConfig",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBClusters"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances"
```



```
    ],
    "Resource" : "arn:aws:rds:*:*:db:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53:ListResourceRecordSets"
    ],
    "Resource" : "arn:aws:route53:::hostedzone/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53:GetHealthCheck",
      "route53:GetHealthCheckStatus"
    ],
    "Resource" : "arn:aws:route53:::healthcheck/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:RequestServiceQuotaIncrease"
    ],
    "Resource" : "arn:aws:servicequotas:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:GetTopicAttributes",
      "sns:ListSubscriptionsByTopic"
    ],
    "Resource" : "arn:aws:sns:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl"
    ],
    "Resource" : "arn:aws:sqs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
"apigateway:GET",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"autoscaling:DescribeAccountLimits",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeAutoScalingInstances",
"autoscaling:DescribeLifecycleHooks",
"autoscaling:DescribeLoadBalancers",
"autoscaling:DescribeLoadBalancerTargetGroups",
"autoscaling:DescribeNotificationConfigurations",
"autoscaling:DescribePolicies",
"cloudwatch:GetMetricData",
"cloudwatch:DescribeAlarms",
"dynamodb:DescribeLimits",
"dynamodb:ListGlobalTables",
"dynamodb:ListTables",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCustomerGateways",
"ec2:DescribeInstances",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetEbsDefaultKmsKeyId",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"kafka:DescribeCluster",
"kafka:DescribeConfigurationRevision",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"rds:DescribeAccountAttributes",
"route53:GetHostedZone",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"sns:GetEndpointAttributes",
"sns:GetSubscriptionAttributes"
],
```

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

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les de de de de de de de de de de de de de de de de de de](#)

Route53ResolverServiceRolePolicy

Route53ResolverServiceRolePolicy est une [politiqueAWS gérée](#) qui : Active l'accès Services AWS aux ressources utilisées ou gérées par Route53 Resolver

des

Cette politique est attachée à un rôle lié au service qui permet à un Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 12 août 2020, 17:47 UTC
- Heure modifiée : 12 août 2020, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version de Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [AWS](#)

S3StorageLensServiceRolePolicy

S3StorageLensServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise l'accès Services AWS aux ressources utilisées ou gérées par S3 Storage Lens

Utilisation des des des de cette politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles

Détails des détails des détails

- Type : Politique de rôles liée à un service

- Heure de création : 18 novembre 2020, 18:15 UTC
- Heure modifiée : 18 novembre 2020, 18:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie Lorsque'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document des d'un document de politique

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec des des desAWS des des des des des des des des des avec des autorisations](#)

SecretsManagerReadWrite

SecretsManagerReadWrite est une [politique AWS gérée](#) qui : fournit un accès en lecture/écriture à AWS Secrets Manager via le. AWS Management Console Remarque : cela exclut les actions IAM, donc combinez-les avec IAM FullAccess si une configuration de rotation est requise.

Utilisation de cette politique

Vous pouvez vous associer SecretsManagerReadWrite à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 avril 2018, 18:05 UTC
- Heure modifiée : 22 février 2024, 18:12 UTC
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
```

```

    "docdb-elastic:GetCluster",
    "docdb-elastic:ListClusters",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "redshift:DescribeClusters",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission",
    "lambda:CreateFunction",
    "lambda:GetFunction",
    "lambda:InvokeFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
},
{
  "Sid" : "SARPermissions",
  "Effect" : "Allow",
  "Action" : [
    "serverlessrepo:CreateCloudFormationChangeSet",
    "serverlessrepo:GetApplication"
  ],
  "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
},
{
  "Sid" : "S3Permissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:s3:::awsserverlessrepo-changesets*",
      "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

SecurityAudit

SecurityAudit est une [politique AWS gérée](#) qui : Le modèle d'audit de sécurité autorise l'accès à la lecture des métadonnées de configuration de sécurité. C'est utile pour les logiciels qui audient la configuration d'un Compte AWS.

Utilisation de cette politique

Vous pouvez vous associer SecurityAudit à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 14 décembre 2023, 21h45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Version de la politique

Version de la politique : v41 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
```

```
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:DescribeVpcIngressConnection",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appsync:GetApiCache",
"appsync:List*",
"athena:GetWorkGroup",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentFrameworkShareRequests",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListControls",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling:Describe*",
"backup:DescribeRegionSettings",
"backup:GetBackupVaultAccessPolicy",
"backup:ListBackupVaults",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobDefinitions",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"chime:List*",
"cloud9:Describe*",
"cloud9:ListEnvironments",
"clouddirectory:ListDirectories",
"cloudformation:DescribeStack*",
"cloudformation:GetStackPolicy",
"cloudformation:GetTemplate",
"cloudformation:ListStack*",
```

```
"cloudfront:Get*",
"cloudfront:List*",
"cloudsearch:DescribeDomainEndpointOptions",
"cloudsearch:DescribeDomains",
"cloudsearch:DescribeServiceAccessPolicies",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrail",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GetDashboard",
"cloudwatch:ListTagsForResource",
"cloudwatch:ListDashboards",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListRepositories",
"codebuild:BatchGetProjects",
"codebuild:ListProjects",
"codecommit:BatchGetRepositories",
"codecommit:GetBranch",
"codecommit:GetObjectIdentifier",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:GetJobDetails",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineExecution",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"codestar:Describe*",
"codestar:List*",
"cognito-identity:Describe*",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:Describe*",
"cognito-idp:ListDevices",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
```

```
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserImportJobs",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"cognito-idp:ListUsers",
"cognito-idp:ListUsersInGroup",
"cognito-sync:Describe*",
"cognito-sync:List*",
"comprehend:Describe*",
"comprehend:List*",
"comprehendmedical:ListICD10CMInferenceJobs",
"comprehendmedical:ListPHIDetectionJobs",
"comprehendmedical:ListRxNormInferenceJobs",
"comprehendmedical:ListSNOMEDCTInferenceJobs",
"config:BatchGetAggregateResourceConfig",
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:SelectAggregateResourceConfig",
"config:SelectResourceConfig",
"connect:ListInstances",
"dataexchange:ListDataSets",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:EvaluateExpression",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ValidatePipelineDefinition",
"datasync:Describe*",
"datasync:List*",
"dax:Describe*",
"dax:ListTags",
"deepracer:ListModels",
"detective:GetGraphIngestState",
"detective:ListGraphs",
"detective:ListMembers",
"devicefarm:ListProjects",
"directconnect:Describe*",
"discovery:DescribeAgents",
"discovery:DescribeConfigurations",
```

```
"discovery:DescribeContinuousExports",
"discovery:DescribeExportConfigurations",
"discovery:DescribeExportTasks",
"discovery:DescribeImportTasks",
"dms:Describe*",
"dms:ListTagsForResource",
"docdb-elastic:ListClusters",
"ds:DescribeDirectories",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetImageBlockPublicAccessState",
"ec2:GetManagedPrefixListAssociations",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImages",
"ecr:DescribeImageScanFindings",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
```

```
"ecr:GetRegistryPolicy",
"ecr:GetRegistryScanningConfiguration",
"ecr:GetRepositoryPolicy",
"ecr:ListImages",
"ecr:ListTagsForResource",
"ecs:Describe*",
"ecs:List*",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodeGroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodeGroups",
"eks:ListUpdates",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elastictranscoder:ListPipelines",
"es:Describe*",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListElasticsearchInstanceTypeDetails",
"es:ListElasticsearchVersions",
"es:ListTags",
"events:Describe*",
"events:List*",
"events:TestEventPattern",
```

```
"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:GetVaultAccessPolicy",
"glacier:GetVaultLock",
"glacier:ListVaults",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:GetCrawlers",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfigurations",
"grafana:ListWorkspaces",
"greengrass:List*",
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
"health:DescribeAffectedEntities",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
"health:DescribeEvents",
"health:DescribeEventTypes",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
```

```
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"iot:Describe*",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:List*",
"iotanalytics:ListChannels",
"iotevents:ListInputs",
"iotfleetwise:ListModelManifests",
"iotsitewise:DescribeGatewayCapabilityConfiguration",
"iotsitewise:ListAssetModels",
"iotsitewise:ListGateways",
"iottwinmaker:ListWorkspaces",
"kafka-cluster:Describe*",
"kafka:Describe*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafkaconnect:Describe*",
"kafkaconnect:List*",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kinesis:DescribeLimits",
"kinesis:DescribeStream",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
```



```
"kinesis:ListShards",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:ListApplications",
"kinesisvideo:DescribeEdgeConfiguration",
"kinesisvideo:DescribeMappedResourceConfiguration",
"kinesisvideo:DescribeMediaStorageConfiguration",
"kinesisvideo:DescribeNotificationConfiguration",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:GetAccountSettings",
"lambda:GetFunctionConfiguration",
"lambda:GetFunctionEventInvokeConfig",
"lambda:GetLayerVersionPolicy",
"lambda:GetPolicy",
"lambda:List*",
"lex:DescribeBot",
"lex:DescribeResourcePolicy",
"lex:ListBots",
"license-manager:List*",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshots",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"machinelearning:DescribeMLModels",
"managedblockchain:ListNetworks",
"mechanicalturk:ListHITs",
"mediaconnect:Describe*",
"mediaconnect:List*",
"medialive:ListChannels",
"mediapackage-vod:DescribePackagingGroup",
```

```
"mediapackage-vod:ListPackagingGroups",
"mediapackage:DescribeOriginEndpoint",
"mediapackage:ListOriginEndpoints",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:ListContainers",
"memorydb:DescribeClusters",
"mq:DescribeBroker",
"mq:DescribeBrokerEngineTypes",
"mq:DescribeBrokerInstanceOptions",
"mq:DescribeConfiguration",
"mq:DescribeConfigurationRevision",
"mq:DescribeUser",
"mq:ListBrokers",
"mq:ListConfigurationRevisions",
"mq:ListConfigurations",
"mq:ListTags",
"mq:ListUsers",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"networkmanager:DescribeGlobalNetworks",
"nimble:ListStudios",
"opsworks-cm:DescribeServers",
"opsworks:DescribeStacks",
"organizations:Describe*",
"organizations:List*",
"personalize:DescribeDatasetGroup",
"personalize:ListDatasetGroups",
"private-networks:ListNetworks",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"quicksight:Describe*",
"quicksight:List*",
"ram:GetResourceShares",
"ram:List*",
```

```
"rds:Describe*",
"rds:DownloadDBLogFilePortion",
"rds:ListTagsForResource",
"redshift:Describe*",
"rekognition:Describe*",
"rekognition:List*",
"resource-groups:ListGroupResources",
"robomaker:Describe*",
"robomaker:List*",
"route53:Get*",
"route53:List*",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
"route53domains:ListDomains",
"route53domains:ListOperations",
"route53domains:ListTagsForDomain",
"route53resolver:Get*",
"route53resolver:List*",
"s3-outposts:ListEndpoints",
"s3-outposts:ListOutpostsWithS3",
"s3-outposts:ListSharedEndpoints",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
```

```
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"schemas:ListSchemaVersions",
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"servicequotas:ListTagsForResource",
"ses:Describe*",
"ses:GetAccountSendingEnabled",
"ses:GetIdentityDkimAttributes",
"ses:GetIdentityPolicies",
"ses:GetIdentityVerificationAttributes",
"ses:ListConfigurationSets",
"ses:ListIdentities",
"ses:ListIdentityPolicies",
"ses:ListReceiptRuleSets",
"ses:ListVerifiedEmailAddresses",
"shield:Describe*",
"shield:GetSubscriptionState",
"shield:List*",
"snowball:ListClusters",
"snowball:ListJobs",
"sns:GetPlatformApplicationAttributes",
```

```
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:ListAssociations",
"ssm:ListAssociationVersions",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocuments",
"ssm:ListDocumentVersions",
"ssm:ListInventoryEntries",
"ssm:ListOpsMetadata",
"ssm:ListResourceComplianceSummaries",
"ssm:ListResourceDataSync",
"ssm:ListTagsForResource",
"sso:DescribeAccountAssignmentCreationStatus",
"sso:DescribePermissionSet",
"sso:DescribePermissionsPolicies",
"sso:List*",
"states:DescribeStateMachine",
"states:ListStateMachines",
"storagegateway:DescribeBandwidthRateLimit",
"storagegateway:DescribeCache",
"storagegateway:DescribeCachediSCSIVolumes",
"storagegateway:DescribeGatewayInformation",
"storagegateway:DescribeMaintenanceStartTime",
"storagegateway:DescribeNFSFileShares",
"storagegateway:DescribeSnapshotSchedule",
"storagegateway:DescribeStorediSCSIVolumes",
"storagegateway:DescribeTapeArchives",
"storagegateway:DescribeTapeRecoveryPoints",
"storagegateway:DescribeTapes",
"storagegateway:DescribeUploadBuffer",
"storagegateway:DescribeVTLDevices",
"storagegateway:DescribeWorkingStorage",
```

```
"storagegateway:List*",
"sts:GetAccessKeyInfo",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
"support:DescribeTrustedAdvisorCheckResult",
"support:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics>ListAssociatedGroups",
"synthetics>ListGroupResources",
"synthetics>ListGroups",
"synthetics>ListTagsForResource",
"tag:GetResources",
"tag:GetTagKeys",
"transcribe:GetCallAnalyticsCategory",
"transcribe:GetMedicalVocabulary",
"transcribe:GetVocabulary",
"transcribe:GetVocabularyFilter",
"transcribe>ListCallAnalyticsCategories",
"transcribe>ListCallAnalyticsJobs",
"transcribe>ListLanguageModels",
"transcribe>ListMedicalTranscriptionJobs",
"transcribe>ListMedicalVocabularies",
"transcribe>ListTagsForResource",
"transcribe>ListTranscriptionJobs",
"transcribe>ListVocabularies",
"transcribe>ListVocabularyFilters",
"transfer:Describe*",
"transfer>List*",
"translate>List*",
"trustedadvisor:Describe*",
"waf-regional:GetWebACL",
"waf-regional>ListResourcesForWebACL",
"waf-regional>ListTagsForResource",
"waf-regional>ListWebACLs",
"waf:GetWebACL",
"waf>ListTagsForResource",
"waf>ListWebACLs",
"wafv2:GetWebACL",
"wafv2:GetWebACLForResource",
```

```

    "wafv2:ListAvailableManagedRuleGroups",
    "wafv2:ListIPSets",
    "wafv2:ListLoggingConfigurations",
    "wafv2:ListRegexPatternSets",
    "wafv2:ListResourcesForWebACL",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "wafv2:ListWebACLs",
    "workdocs:DescribeResourcePermissions",
    "workspaces:Describe*",
    "xray:GetEncryptionConfig",
    "xray:GetGroup",
    "xray:GetGroups",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetTraceSummaries",
    "xray:ListTagsForResource"
  ]
},
{
  "Effect" : "Allow",
  "Sid" : "APIGatewayAccess",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis",
    "arn:aws:apigateway:*::/apis/*/authorizers/*",
    "arn:aws:apigateway:*::/apis/*/authorizers",
    "arn:aws:apigateway:*::/apis/*/cors",
    "arn:aws:apigateway:*::/apis/*/deployments/*",
    "arn:aws:apigateway:*::/apis/*/deployments",
    "arn:aws:apigateway:*::/apis/*/exports/*",
    "arn:aws:apigateway:*::/apis/*/integrations/*",
    "arn:aws:apigateway:*::/apis/*/integrations",
    "arn:aws:apigateway:*::/apis/*/models/*",
    "arn:aws:apigateway:*::/apis/*/models",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/apis/*/stages",
    "arn:aws:apigateway:*::/apis/*/stages/*",
    "arn:aws:apigateway:*::/clientcertificates",
    "arn:aws:apigateway:*::/clientcertificates/*",
    "arn:aws:apigateway:*::/domainnames",
  ]
}

```

```

    "arn:aws:apigateway:*::/domainnames/*/apimappings",
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/authorizers/*",
    "arn:aws:apigateway:*::/restapis/*/authorizers",
    "arn:aws:apigateway:*::/restapis/*/deployments/*",
    "arn:aws:apigateway:*::/restapis/*/deployments",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
    "arn:aws:apigateway:*::/restapis/*/models/*",
    "arn:aws:apigateway:*::/restapis/*/models",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/tags/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

SecurityLakeServiceLinkedRole

SecurityLakeServiceLinkedRole est une [politique AWS gérée](#) qui : Cette politique accorde les autorisations nécessaires pour exploiter le service Amazon Security Lake en votre nom

Utilisation de cette politique

Cette politique est associée à un rôle lié au service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : Politique de rôle liée à un service
- Heure de création : 29 novembre 2022, 14:03 UTC
- Heure modifiée : 29 février 2024, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```

    "Action" : [
      "organizations:DescribeAccount"
    ],
    "Resource" : [
      "arn:aws:organizations::*:account/o-*/*"
    ]
  },
  {
    "Sid" : "AllowManagementOfServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail>DeleteServiceLinkedChannel",
      "cloudtrail:GetServiceLinkedChannel",
      "cloudtrail:UpdateServiceLinkedChannel"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
  },
  {
    "Sid" : "AllowListServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DescribeAnyVpc",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListDelegatedAdmins",
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
      }
    }
  }

```

```
    }
  }
},
{
  "Sid" : "AllowWafLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "wafv2:LogScope" : "SecurityLake"
    }
  }
},
{
  "Sid" : "AllowPutLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
    }
  }
},
{
  "Sid" : "ListWebACLs",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:ListWebACLs"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège](#)

ServerMigration_ServiceRole

ServerMigration_ServiceRole est une [politique AWS gérée](#) qui : Autorisations permettant au service de migration de AWS serveurs de migrer des machines virtuelles vers EC2 : autorise le service de migration de serveurs à placer les ressources migrées sur le compte EC2 du client.

Utilisation de cette stratégie

Vous pouvez ServerMigration_ServiceRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 11 août 2020, 20:41 UTC
- Heure modifiée : 15 octobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```

    "cloudformation:CreateChangeSet",
    "cloudformation:CreateStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**",
  "Condition" : {
    "Null" : {
      "cloudformation:ResourceTypes" : "false"
    },
    "ForAllValues:StringEquals" : {
      "cloudformation:ResourceTypes" : [
        "AWS::EC2::Instance",
        "AWS::ApplicationInsights::Application",
        "AWS::ResourceGroups::Group"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:DeleteChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:GetTemplate"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",

```

```

    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*::document/AWS-RunRemoteScript",
    "arn:aws:s3:::sms-app-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CopySnapshot"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CopySnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  }
]
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DeregisterImage",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",

```



```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    },
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "cloudformation.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServerMigrationConnector

ServerMigrationConnector est une [politiqueAWS gérée](#) qui : Autorisations permettant au connecteur de migration deAWS serveur de migrer des machines virtuelles vers EC2. Permet la communication avec le service de migration deAWS serveurs, l'accès en lecture/écriture aux compartiments S3 commençant par « sms-b- » et « import-to-ec 2 », ainsi qu'aux compartiments utilisés pour la mise à niveau du connecteur de migrationAWS du serveur, l'enregistrement du connecteur de migrationAWS du serveur auprèsAWS de celui-ci et le téléchargement des métriques vers lequel les métriques sont téléchargéesAWS.

Utilisation de cette stratégie

Vous pouvez les associer `ServerMigrationConnector` à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 octobre 2016, 21:45 UTC
- Heure modifiée : 24 octobre 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "s3:CreateBucket",
      "s3>DeleteBucket",
      "s3>DeleteObject",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutLifecycleConfiguration",
      "s3:AbortMultipartUpload",
      "s3:ListBucketMultipartUploads",
      "s3:ListMultipartUploadParts"
    ],
    "Resource" : [
      "arn:aws:s3:::sms-b-*",
      "arn:aws:s3:::import-to-ec2-*",
      "arn:aws:s3:::server-migration-service-upgrade",
      "arn:aws:s3:::server-migration-service-upgrade/*",
      "arn:aws:s3:::connector-platform-upgrade-info/*",
      "arn:aws:s3:::connector-platform-upgrade-info",
      "arn:aws:s3:::connector-platform-upgrade-bundles/*",
      "arn:aws:s3:::connector-platform-upgrade-bundles",
      "arn:aws:s3:::connector-platform-release-notes/*",
      "arn:aws:s3:::connector-platform-release-notes"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "awsconnector:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "SNS:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression des autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrez avec les stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServerMigrationServiceConsoleFullAccess

ServerMigrationServiceConsoleFullAccess est une [politiqueAWS gérée](#) qui : Autorisations requises pour utiliser toutes les fonctionnalités de la console du service de migration des serveurs

Utilisation de cette stratégie

Vous pouvez ServerMigrationServiceConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 9 mai 2020, 17:18 UTC
- Heure modifiée : 20 juillet 2020, 22h00 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

```
{
  "Action" : [
    "sms:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "cloudformation:ListStacks",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "s3:ListAllMyBuckets",
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "arn:aws:s3:::sms-app-*/*"
},
{
  "Action" : [
    "ec2:DescribeKeyPairs",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
```

```
"Action" : [
  "iam:CreateServiceLinkedRole"
],
"Condition" : {
  "StringEquals" : {
    "iam:AWSServiceName" : "sms.amazonaws.com"
  }
},
"Effect" : "Allow",
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetInstanceProfile",
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole est une [politique AWS gérée](#) qui : Autorisations permettant au service de migration de AWS serveurs de créer et de mettre à jour les AWS ressources pertinentes dans celles du client Compte AWS pour lancer des serveurs et des applications migrés.

Utilisation de cette stratégie

Vous pouvez ServerMigrationServiceLaunchRole les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service

- Heure de création : 26 novembre 2018, 19:53 UTC
- Heure modifiée : 15 octobre 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
            "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:DisassociateIamInstanceProfile",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*",
      "cloudformation:ListStackResources",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [

```



```

        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights>DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights>DeleteComponent"
    ],
    "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
        "Effect" : "Allow",
        "Action" : [
            "resource-groups:CreateGroup",
            "resource-groups:GetGroup",
            "resource-groups:UpdateGroup",
            "resource-groups>DeleteGroup"
        ],
        "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
        "Condition" : {
            "StringLike" : {
                "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
            }
        }
    },
    {
        "Effect" : "Allow",
        "Action" : [
            "iam:CreateServiceLinkedRole"
        ],
        "Resource" : [
            "arn:aws:iam:*:*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
        ],
        "Condition" : {
            "StringEquals" : {
                "iam:AWSServiceName" : "application-insights.amazonaws.com"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServerMigrationServiceRoleForInstanceValidation

ServerMigrationServiceRoleForInstanceValidation est une [politiqueAWS gérée](#) qui :
Autorisations permettant auAWS SMS d'exécuter le script de validation des données utilisé et de renvoyer la réussite ou l'échec du script au SMS

Utilisation de cette stratégie

Vous pouvezServerMigrationServiceRoleForInstanceValidation les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 20 juillet 2020, 22:25 UTC
- Heure modifiée : 20 juillet 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3:::sms-app-*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "sms:NotifyAppValidationOutput",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServiceQuotasFullAccess

ServiceQuotasFullAccess est une [politiqueAWS gérée](#) qui : Fournit un accès complet aux Service Quotas

Utilisation de cette stratégie

Vous pouvezServiceQuotasFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 24 juin 2019, 15:44 UTC
- Heure modifiée : 4 février 2021, 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

Version de la politique

Version de la politique :v4 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
    }
  ]
}
```

```
"Resource" : "*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/ServiceQuotaMonitor" : "false"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "servicequotas.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "servicequotas.amazonaws.com"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServiceQuotasReadOnlyAccess

ServiceQuotasReadOnlyAccess est une [politique AWS gérée](#) qui : Fournit un accès en lecture seule aux Service Quotas

Utilisation de cette stratégie

Vous pouvez ServiceQuotasReadOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 24 juin 2019, 15:31 UTC
- Heure modifiée : 21 décembre 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
```

```

    "dynamodb:DescribeLimits",
    "elasticloadbalancing:DescribeAccountLimits",
    "iam:GetAccountSummary",
    "kinesis:DescribeLimits",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "rds:DescribeAccountAttributes",
    "route53:GetAccountLimit",
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "servicequotas:GetAssociationForServiceQuotaTemplate",
    "servicequotas:GetAWSDefaultServiceQuota",
    "servicequotas:GetRequestedServiceQuotaChange",
    "servicequotas:GetServiceQuota",
    "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
    "servicequotas:ListAWSDefaultServiceQuotas",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
    "servicequotas:ListServices",
    "servicequotas:ListServiceQuotas",
    "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
    "servicequotas:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

ServiceQuotasServiceRolePolicy

ServiceQuotasServiceRolePolicyest une [politiqueAWS gérée](#) qui : Autorise Service Quotas à créer des dossiers de support en votre nom

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

SimpleWorkflowFullAccess

SimpleWorkflowFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet au service de configuration Simple Workflow.

Utilisation de cette stratégie

Vous pouvez SimpleWorkflowFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 6 février 2015, 18:41 UTC
- Heure modifiée : 6 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

SupportUser

SupportUser est une [AWS politique gérée](#) : cette politique accorde les autorisations nécessaires pour dépanner et résoudre les problèmes dans un Compte AWS. Cette politique permet également à l'utilisateur de contacter l'assistance AWS pour créer et gérer des dossiers.

Utilisation de cette politique

Vous pouvez joindre SupportUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type: Politique relative aux fonctions professionnelles
- Heure de création: 10 novembre 2016, 17:21 UTC
- Heure modifiée :25 août 2023, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

Version de la politique

Version de la politique : v8(par défaut)

La version par défaut de la politique est celle qui définit les autorisations associées à la politique. Lorsqu'un utilisateur ou un rôle associé à la politique fait une demande d'accès à

unAWSresource,AWSvérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
```

```
"codepipeline:ListActionTypes",
"codepipeline:ListPipelines",
"codepipeline:PollForJobs",
"codepipeline:PollForThirdPartyJobs",
"codepipeline:GetPipelineState",
"codepipeline:GetPipeline",
"cognito-identity:List*",
"cognito-identity:LookupDeveloperIdentity",
"cognito-identity:Describe*",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeRiskConfiguration",
"cognito-idp:DescribeUserImportJob",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:List*",
"cognito-sync:Describe*",
"cognito-sync:GetBulkPublishDetails",
"cognito-sync:GetCognitoEvents",
"cognito-sync:GetIdentityPoolConfiguration",
"cognito-sync:List*",
"config:DescribeConfigurationRecorders",
"config:DescribeConfigurationRecorderStatus",
"config:DescribeConfigRuleEvaluationStatus",
"config:DescribeConfigRules",
"config:DescribeDeliveryChannels",
"config:DescribeDeliveryChannelStatus",
"config:GetResourceConfigHistory",
"config:ListDiscoveredResources",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ReportTaskProgress",
"datapipeline:ReportTaskRunnerHeartbeat",
"devicefarm:List*",
"devicefarm:Get*",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:ListConfigurations",
"dms:Describe*",
"dms:List*",
"ds:DescribeDirectories",
"ds:DescribeSnapshots",
```

```
"ds:GetDirectoryLimits",
"ds:GetSnapshotLimits",
"ds:ListAuthorizedApplications",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"ec2:Describe*",
"ec2:DescribeHosts",
"ec2:describeIdentityIdFormat",
"ec2:DescribeIdFormat",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeNatGateways",
"ec2:DescribeReservedInstancesModifications",
"ec2:DescribeTags",
"ec2:SearchLocalGatewayRoutes",
"ecr:GetRepositoryPolicy",
"ecr:BatchCheckLayerAvailability",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticbeanstalk:ValidateConfigurationSettings",
"elasticfilesystem:Describe*",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:List*",
"elastictranscoder:List*",
"elastictranscoder:ReadJob",
"elasticfilesystem:DescribeFileSystems",
"es:Describe*",
"es:List*",
"es:ESHttpGet",
"es:ESHttpHead",
"events:DescribeRule",
"events:List*",
"events:TestEventPattern",
"firehose:Describe*",
```

```
"firehose:List*",
"gamelift:List*",
"gamelift:Describe*",
"glacier:ListVaults",
"glacier:DescribeVault",
"glacier:DescribeJob",
"glacier:Get*",
"glacier:List*",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"importexport:GetStatus",
"importexport:ListJobs",
"inspector:Describe*",
"inspector:List*",
"iot:Describe*",
"iot:Get*",
"iot:List*",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:DiscoverInputSchema",
"kinesisanalytics:GetApplicationState",
"kinesisanalytics:ListApplications",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:List*",
"lambda:Get*",
"logs:Describe*",
"logs:TestMetricFilter",
"machinelearning:Describe*",
"machinelearning:Get*",
"opsworks:Describe*",
"rds:Describe*",
"rds:ListTagsForResource",
"redshift:Describe*",
"route53:Get*",
"route53:List*",
"route53domains:CheckDomainAvailability",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
```

```
    "route53domains:List*",
    "s3:List*",
    "sdb:GetAttributes",
    "sdb:List*",
    "sdb:Select*",
    "servicecatalog:SearchProducts",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ScanProvisionedProducts",
    "ses:Get*",
    "ses:List*",
    "sns:Get*",
    "sns:List*",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "sqs:ListQueues",
    "sqs:ReceiveMessage",
    "ssm:List*",
    "ssm:Describe*",
    "storagegateway:Describe*",
    "storagegateway:List*",
    "swf:Count*",
    "swf:Describe*",
    "swf:Get*",
    "swf:List*",
    "waf:Get*",
    "waf:List*",
    "workdocs:Describe*",
    "workmail:Describe*",
    "workmail:Get*",
    "workspaces:Describe*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

En savoir plus

- [Créez un ensemble d'autorisations à l'aide deAWSpolitiques gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement des politiques IAM](#)
- [Commencez avecAWSpolitiques gérées et évolution vers les autorisations du moindre privilège](#)

SystemAdministrator

SystemAdministrator est une [politiqueAWS gérée](#) qui : accorde les autorisations d'accès complètes nécessaires aux ressources requises pour les opérations d'application et de développement.

Utilisation de cette stratégie

Vous pouvezSystemAdministrator les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique relative aux fonctions Job
- Heure de création : 10 novembre 2016, 17:23 UTC
- Heure modifiée : 24 août 2020, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Version de la politique

Version de la politique :v6 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Statement" : [
    {
```



```
"Action" : [  
  "acm:Describe*",  
  "acm:Get*",  
  "acm:List*",  
  "acm:Request*",  
  "acm:Resend*",  
  "autoscaling:*",  
  "cloudtrail:DescribeTrails",  
  "cloudtrail:GetTrailStatus",  
  "cloudtrail:ListPublicKeys",  
  "cloudtrail:ListTags",  
  "cloudtrail:LookupEvents",  
  "cloudtrail:StartLogging",  
  "cloudtrail:StopLogging",  
  "cloudwatch:*",  
  "codecommit:BatchGetRepositories",  
  "codecommit:CreateBranch",  
  "codecommit:CreateRepository",  
  "codecommit:Get*",  
  "codecommit:GitPull",  
  "codecommit:GitPush",  
  "codecommit:List*",  
  "codecommit:Put*",  
  "codecommit:Test*",  
  "codecommit:Update*",  
  "codedeploy:*",  
  "codepipeline:*",  
  "config:*",  
  "ds:*",  
  "ec2:Allocate*",  
  "ec2:AssignPrivateIpAddresses*",  
  "ec2:Associate*",  
  "ec2:Allocate*",  
  "ec2:AttachInternetGateway",  
  "ec2:AttachNetworkInterface",  
  "ec2:AttachVpnGateway",  
  "ec2:Bundle*",  
  "ec2:Cancel*",  
  "ec2:Copy*",  
  "ec2:CreateCustomerGateway",  
  "ec2:CreateDhcpOptions",  
  "ec2:CreateFlowLogs",  
  "ec2:CreateImage",  
  "ec2:CreateInstanceExportTask",
```

```
"ec2:CreateInternetGateway",
"ec2:CreateKeyPair",
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:CreateNatGateway",
"ec2:CreateNetworkInterface",
"ec2:CreatePlacementGroup",
"ec2:CreateReservedInstancesListing",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateSpotDatafeedSubscription",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteKeyPair",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkInterface",
"ec2>DeletePlacementGroup",
"ec2>DeleteSnapshot",
"ec2>DeleteSpotDatafeedSubscription",
"ec2>DeleteSubnet",
"ec2>DeleteTags",
"ec2>DeleteVpc",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteVpnConnection",
"ec2>DeleteVpnConnectionRoute",
"ec2>DeleteVpnGateway",
"ec2:DeregisterImage",
"ec2:Describe*",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
```

```
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVolumeIO",
"ec2:EnableVpcClassicLinkDnsSupport",
"ec2:GetConsoleOutput",
"ec2:GetHostReservationPurchasePreview",
"ec2:GetLaunchTemplateData",
"ec2:GetPasswordData",
"ec2:Import*",
"ec2:Modify*",
"ec2:MonitorInstances",
"ec2:MoveAddressToVpc",
"ec2:Purchase*",
"ec2:RegisterImage",
"ec2:Release*",
"ec2:Replace*",
"ec2:ReportInstanceStatus",
"ec2:Request*",
"ec2:Reset*",
"ec2:RestoreAddressToClassic",
"ec2:RunScheduledInstances",
"ec2:UnassignPrivateIpAddresses",
"ec2:UnmonitorInstances",
"ec2:UpdateSecurityGroupRuleDescriptionsEgress",
"ec2:UpdateSecurityGroupRuleDescriptionsIngress",
"elasticloadbalancing:*",
"events:*",
"iam:GetAccount*",
"iam:GetContextKeys*",
"iam:GetCredentialReport",
"iam:ListAccountAliases",
"iam:ListGroups",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListPoliciesGrantingServiceAccess",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:Simulate*",
"iam:UpdateServerCertificate",
"iam:UpdateSigningCertificate",
"kinesis:ListStreams",
"kinesis:PutRecord",
```

```
    "kms:CreateAlias",
    "kms:CreateKey",
    "kms>DeleteAlias",
    "kms:Describe*",
    "kms:GenerateRandom",
    "kms:Get*",
    "kms:List*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "lambda:Create*",
    "lambda>Delete*",
    "lambda:Get*",
    "lambda:InvokeFunction",
    "lambda:List*",
    "lambda:PublishVersion",
    "lambda:Update*",
    "logs:*",
    "rds:Describe*",
    "rds:ListTagsForResource",
    "route53:*",
    "route53domains:*",
    "ses:*",
    "sns:*",
    "sqs:*",
    "trustedadvisor:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "ec2:AcceptVpcPeeringConnection",
    "ec2:AttachClassicLinkVpc",
    "ec2:AttachVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateVpcPeeringConnection",
    "ec2>DeleteCustomerGateway",
    "ec2>DeleteDhcpOptions",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteNetworkAcl*",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2>DeleteSecurityGroup",
```

```

    "ec2:DeleteVolume",
    "ec2:DeleteVpcPeeringConnection",
    "ec2:DetachClassicLinkVpc",
    "ec2:DetachVolume",
    "ec2:DisableVpcClassicLink",
    "ec2:EnableVpcClassicLink",
    "ec2:GetConsoleScreenshot",
    "ec2:RebootInstances",
    "ec2:RejectVpcPeeringConnection",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "s3:*",
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "iam:GetAccessKeyLastUsed",
    "iam:GetGroup*",
    "iam:GetInstanceProfile",
    "iam:GetLoginProfile",
    "iam:GetOpenIDConnectProvider",
    "iam:GetPolicy*",
    "iam:GetRole*",
    "iam:GetSAMLProvider",
    "iam:GetSSHPublicKey",
    "iam:GetServerCertificate",
    "iam:GetServiceLastAccessed*",
    "iam:GetUser*",
    "iam:ListAccessKeys",
    "iam:ListAttached*",

```

```

    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroupsForUser",
    "iam:ListInstanceProfiles*",
    "iam:ListMFADevices",
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "iam:ListSSHPublicKeys",
    "iam:ListSigningCertificates",
    "iam:ListUserPolicies",
    "iam:Upload*"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/rds-monitoring-role",
    "arn:aws:iam::*:role/ec2-sysadmin-*",
    "arn:aws:iam::*:role/ecr-sysadmin-*",
    "arn:aws:iam::*:role/lambda-sysadmin-*"
  ]
}
],
"Version" : "2012-10-17"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

TranslateFullAccess

TranslateFullAccess est une [politique AWS gérée](#) qui : Fournit un accès complet à Amazon Translate.

Utilisation de cette stratégie

Vous pouvez TranslateFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 23:36 UTC
- Heure modifiée : 8 janvier 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec les stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

TranslateReadOnly

TranslateReadOnly est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon Translate.

Utilisation de cette stratégie

Vous pouvez l'associer TranslateReadOnly à vos utilisateurs, à vos groupes et à vos rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 18:22 UTC
- Heure modifiée : 24 mai 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

ViewOnlyAccess

ViewOnlyAccess est une [politique AWS gérée](#) qui : Cette politique autorise l'affichage des ressources et des métadonnées de base pour tous les AWS services.

Utilisation de cette stratégie

Vous pouvez ViewOnlyAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique relative aux fonctions Job
- Heure de création : 10 novembre 2016, 17:20 UTC
- Heure modifiée : 6 mars 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Version de la politique

Version de la politique :v17 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "batch:ListJobs",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudhsm:ListAvailableZones",
        "cloudhsm:ListHapgs",
        "cloudhsm:ListHsms",
        "cloudhsm:ListLunaClients",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",

```

```
"cloudtrail:DescribeTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"codebuild:ListBuilds*",
"codebuild:ListProjects",
"codecommit:List*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:ListPipelines",
"codestar:List*",
"cognito-identity:ListIdentities",
"cognito-identity:ListIdentityPools",
"cognito-idp:List*",
"cognito-sync:ListDatasets",
"config:Describe*",
"config:List*",
"connect:List*",
"comprehend:Describe*",
"comprehend:List*",
"datapipeline:DescribePipelines",
"datapipeline:GetAccountLimits",
"datapipeline:ListPipelines",
"dax:DescribeClusters",
"dax:DescribeDefaultParameters",
"dax:DescribeEvents",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"devicefarm:List*",
"directconnect:Describe*",
"discovery:List*",
"dms:List*",
"ds:DescribeDirectories",
"dynamodb:DescribeBackup",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeReservedCapacity",
"dynamodb:DescribeReservedCapacityOfferings",
"dynamodb:DescribeStream",
"dynamodb:DescribeTable",
```

```
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeBundleTasks",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeExportTasks",
"ec2:DescribeFlowLogs",
"ec2:DescribeHost*",
"ec2:DescribeIdFormat",
"ec2:DescribeIdentityIdFormat",
"ec2:DescribeImage*",
"ec2:DescribeImport*",
"ec2:DescribeInstance*",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeLocalGatewayRouteTables",
"ec2:DescribeLocalGatewayVirtualInterfaceGroups",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeLocalGateways",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetwork*",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeReserved*",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshot*",
"ec2:DescribeSpot*",
"ec2:DescribeSubnets",
```

```
"ec2:DescribeTags",
"ec2:DescribeVolume*",
"ec2:DescribeVpc*",
"ec2:DescribeVpnGateways",
"ec2:SearchLocalGatewayRoutes",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeEnvironments",
"elasticbeanstalk:ListAvailableSolutionStacks",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:List*",
"elastictranscoder:List*",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
"events:ListRuleNamesByTarget",
"events:ListRules",
"events:ListTargetsByRule",
"firehose:DescribeDeliveryStream",
"firehose:List*",
"fsx:DescribeFileSystems",
"gamelift:List*",
"glacier:List*",
"greengrass:List*",
"iam:GetAccountSummary",
"iam:GetLoginProfile",
"iam:List*",
"importexport:ListJobs",
"inspector:List*",
"iot:List*",
```

```
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kms:ListKeys",
"lambda:List*",
"lex:GetBotAliases",
"lex:GetBotChannelAssociations",
"lex:GetBotVersions",
"lex:GetBots",
"lex:GetIntentVersions",
"lex:GetIntents",
"lex:GetSlotTypeVersions",
"lex:GetSlotTypes",
"lex:GetUtterancesView",
"lightsail:GetBlueprints",
"lightsail:GetBundles",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetRegions",
"lightsail:GetStaticIps",
"lightsail:IsVpcPeered",
"logs:Describe*",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"machinelearning:Describe*",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetImportJobs",
"mobiletargeting:GetSegments",
"opsworks-cm:Describe*",
"opsworks:Describe*",
"organizations:List*",
"outposts:GetOutpost",
"outposts:GetOutpostInstanceTypes",
"outposts:ListOutposts",
"outposts:ListSites",
"outposts:ListTagsForResource",
"polly:Describe*",
"polly:List*",
```

```
"rds:Describe*",
"redshift:DescribeClusters",
"redshift:DescribeEvents",
"redshift:ViewQueriesInConsole",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"route53:Get*",
"route53:List*",
"route53domains:List*",
"route53resolver:Get*",
"route53resolver:List*",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"sagemaker:Describe*",
"sagemaker:List*",
"sdb:List*",
"servicecatalog:List*",
"ses:List*",
"shield:List*",
"sns:List*",
"sqs:ListQueues",
"ssm:ListAssociations",
"ssm:ListDocuments",
"states:ListActivities",
"states:ListStateMachines",
"storagegateway:ListGateways",
"storagegateway:ListLocalDisks",
"storagegateway:ListVolumeRecoveryPoints",
"storagegateway:ListVolumes",
"swf:List*",
"trustedadvisor:Describe*",
"waf-regional:List*",
"waf:List*",
"wafv2:List*",
"workdocs:DescribeAvailableDirectories",
"workdocs:DescribeInstances",
"workmail:Describe*",
"workspaces:Describe*"
],
"Effect" : "Allow",
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector` est une [politiqueAWS gérée](#) qui : Stratégie par défaut pour le rôle de service VM Import/Export, pour les clients utilisant leAWS Connector. Le service VM Import/Export joue un rôle dans le cadre de cette politique pour répondre aux demandes de migration de machines virtuelles provenant du dispositif virtuelAWS Connector. (Notez que leAWS Connector utilise la politique géréeAWSConnector « » pour envoyer des demandes au nom du client au service VM Import/Export.) Permet de créer des AMI et des instantanés EBS, de modifier les attributs des instantanés EBS, de lancer des appels « Describe* » sur des objets EC2 et de lire à partir de compartiments S3 en commençant par «import-to-ec 2 ».

Utilisation de cette stratégie

Vous pouvez `VMImportExportRoleForAWSConnector` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : Politique de rôle de service
- Heure de création : 3 septembre 2015, 20:48 UTC
- Heure modifiée : 3 septembre 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

VPCLatticeFullAccess

VPCLatticeFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet à Amazon VPC Lattice et un accès aux services de dépendance.

Utilisation de cette stratégie

Vous pouvezVPCLatticeFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 mars 2023, 02:49 UTC
- Heure modifiée : 30 mars 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
```

```

    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeLoadBalancers",
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams",
    "logs:DescribeLogGroups",
    "s3:ListAllMyBuckets",
    "lambda:ListAliases",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:GetLogDelivery",
    "logs:ListLogDeliveries",
    "logs:UpdateLogDelivery",
    "logs:DescribeResourcePolicies"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "vpc-lattice.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/AWSServiceRoleForVpcLattice",
  "Condition" : {
    "StringLike" : {

```

```

        "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

VPCLatticeReadOnlyAccess

VPCLatticeReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à Amazon VPC Lattice via les AWS Management Console services de dépendance et un accès limité à ceux-ci.

Utilisation de cette stratégie

Vous pouvez `VPCLatticeReadOnlyAccess` les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politique AWS gérée
- Heure de création : 30 mars 2023, 02:47 UTC
- Heure modifiée : 30 mars 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
```

```
    "firehose:ListDeliveryStreams",
    "lambda:ListAliases",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction",
    "logs:DescribeLogGroups",
    "logs:GetLogDelivery",
    "logs:ListLogDeliveries",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

VPCLatticeServicesInvokeAccess

VPCLatticeServicesInvokeAccess est une [politiqueAWS gérée](#) qui : Fournit l'accès à l'appel des services Amazon VPC Lattice.

Utilisation de cette stratégie

Vous pouvezVPCLatticeServicesInvokeAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 30 mars 2023, 02:45 UTC
- Heure modifiée : 30 mars 2023, 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

WAFLoggingServiceRolePolicy

WAFLoggingServiceRolePolicyest une [politiqueAWS gérée](#) qui : Création d'un SLR pour enregistrer les journaux des clients dans un flux Firehose

Utilisation de cette politique en utilisation de

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques,

- Type : Politique de rôles liée à un service
- Heure de création : 24 août 2018, 21:05 UTC
- Heure modifiée : 24 août 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON politique J

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège des politiques gérées et évoluez vers les autorisations de moindre privilège](#)

WAFRegionalLoggingServiceRolePolicy

WAFRegionalLoggingServiceRolePolicy est une [politique AWS gérée](#) qui : Création d'un SLR pour enregistrer les journaux des clients dans un flux Firehose

Utilisation de politique

Cette politique est attachée à un rôle lié au service qui permet à d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, les groupes ou les rôles.

Détails des politique

- Type : Politique de rôles liée à un service
- Heure de création : 24 août 2018, 18:40 UTC
- Heure modifiée : 24 août 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par politique est la version qui définit les autorisations. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
```

```
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"  
    ]  
}  
]  
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiques AWS gérées et évoluez vers les autorisations de moindre privilège](#)

WAFV2LoggingServiceRolePolicy

WAFV2LoggingServiceRolePolicy est une [politique AWS gérée](#) qui : Cette politique crée un rôle lié à un service qui permet à AWS WAF d'écrire des journaux dans Amazon Kinesis Data Firehose.

Utilisation de cette politique

Cette politique est attachée à un rôle lié au service qui permet à un service d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos utilisateurs, groupes ou rôles.

Les détails des politiques

- Type : Politique de rôles liée à un service
- Heure de création : 7 novembre 2019, 00:40 UTC
- Heure modifiée : 23 juillet 2020, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Version de la politique

Version de la politique :v2 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec politiquesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

WellArchitectedConsoleFullAccess

WellArchitectedConsoleFullAccess est une [politiqueAWS gérée](#) qui : fournit un accès complet àAWS Well-Architected Tool via leAWS Management Console

Utilisation de cette stratégie

Vous pouvezWellArchitectedConsoleFullAccess les associer à vos utilisateurs, groupes et rôles.

Détails des politiques

- Type : politiqueAWS gérée
- Heure de création : 29 novembre 2018, 18:19 UTC
- Heure modifiée : 29 novembre 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à uneAWS ressource,AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiquesAWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations basées sur l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarrer avec stratégiesAWS gérées et évoluez vers les autorisations de moindre privilège](#)

WellArchitectedConsoleReadOnlyAccess

WellArchitectedConsoleReadOnlyAccess est une [politique AWS gérée](#) qui : fournit un accès en lecture seule à l'outil AWS Well-Architected via AWS Management Console

Utilisation de cette politique

Vous pouvez l'associer WellArchitectedConsoleReadOnlyAccess à vos utilisateurs, à vos groupes et à vos rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 18:21 UTC
- Heure modifiée : 29 juin 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de politique JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre le versionnement pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations de moindre privilège](#)

WorkLinkServiceRolePolicy

WorkLinkServiceRolePolicy est une [politique AWS gérée](#) qui : Autorise l'accès Services AWS aux ressources utilisées ou gérées par Amazon WorkLink

Utilisation de cette stratégie

Vous pouvez WorkLinkServiceRolePolicy les associer à vos utilisateurs, groupes et rôles.

Détails des stratégies

- Type : politique AWS gérée
- Heure de création : 23 janvier 2019, 19:03 UTC
- Heure modifiée : 23 janvier 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Version de la politique

Version de la politique :v1 (par défaut)

La version par défaut de la stratégie est la version qui définit les autorisations pour la stratégie. Lorsqu'un utilisateur ou un rôle doté de la politique demande l'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser la demande.

Document de stratégie JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:CreateNetworkInterfacePermission",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2>DeleteNetworkInterface"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:PutRecord",
      "kinesis:PutRecords"
    ],
    "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajout et suppression d'autorisations pour l'identité IAM](#)
- [Comprendre le contrôle des versions pour les politiques IAM](#)
- [Démarez avec stratégies AWS gérées et évoluez vers les autorisations de moindre privilège](#)

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.